In the matter of the General Data Protection Regulation

DPC Case Reference: IN-21-3-2

In the matter of the Department of Health

Decision of the Data Protection Commission made pursuant to section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to section 110 of the Data Protection Act 2018

DECISION

Decision-Maker for the Data Protection Commission:

_____

Helen Dixon
Commissioner for Data Protection

16 June 2023

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1. This document (the '**Decision**') is a decision made by the Data Protection Commission (the '**DPC'**) in accordance with section 111 of the Data Protection Act 2018 (the '**2018 Act**'). I make this Decision having considered the information obtained in the own volition inquiry ('**the Inquiry**') pursuant to section 110 of the 2018 Act.

1.2. The inquiry team of the DPC (the '**Case Officers**') provided the Department of Health (the '**DOH**') with an Inquiry Issues Paper in order to allow it to make submissions. An initial draft decision (the '**Draft Decision**') was provided to the DOH on 9 December 2021. The DOH sent its submissions on the Draft Decision on 9 March 2022. A revised draft decision (the '**Revised Draft Decision**') was provided to the DOH on 3 May 2023 to give it a final opportunity to make any further submissions. As decision-maker, I have fully considered the submissions made by the DOH.

1.3. This Decision contains corrective powers under section 115 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (the '**GDPR**') arising from the infringements which have been identified herein. It should be noted, in this regard, that the DOH is required to comply with any corrective powers contained in this Decision, and it is open to this office to serve an enforcement notice on the DOH in accordance with section 133 of the 2018 Act.

2. Legal Framework for the Inquiry and the Decision

i. Legal Basis for the Inquiry

2.1. The GDPR is the legal regime covering the processing of personal data in the European Union ('**EU**'). As a regulation, the GDPR is directly applicable in EU member states ('**Member States**'). The GDPR is given further effect in Irish law by the 2018 Act. As stated above, the Inquiry was commenced pursuant to section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the DPC has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.

2.2. Section 110(1) of the 2018 Act provides that the DPC may, for the purpose of section 109(5)(e) or section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or a regulation under the Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the DPC may, for the purposes of section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

ii. Controller

2.3. This Decision relates to personal data in respect of which the DOH is the controller, within the meaning of Article 4(7) GDPR.

iii. Legal Basis for the Decision

2.4. The decision-making process for the Inquiry which applies to this case is provided for under section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. As the sole member of the DPC as defined in section 15 of the 2018 Act, I perform this function in my role as the decision-maker in the DPC. In so doing, I am required to assess all of the materials and submissions gathered during the Inquiry and any other materials that I consider to be relevant, in the course of the decision-making process.

2.5. A full schedule of all documentation considered by me for the purpose of the preparation of this Decision is appended hereto. Having considered the information obtained in the Inquiry, I am satisfied that the Inquiry has been correctly conducted and that fair procedures have been followed throughout. I also had regard to the submissions that the DOH made before proceeding to make a final Decision under section 111 of the 2018 Act.

3. Factual Background

3.1. The DOH is a government department whose overall mission is to improve the health and wellbeing of people in Ireland. The DOH sets policy in relation to specialist community disability services, which aim to ensure the delivery of person centred supports to enable those with a disability to live ordinary lives in their community. This includes setting policy relating to the delivery of health services to children with special education needs (‘**SEN’** or **‘SENs’**), to support those children to access education that is appropriate to their needs.

3.2. In March 2021, the DPC became aware of allegations made publicly against DOH. The allegations were made by a DOH staff member (the ‘**Whistleblower**’). They concerned the manner in which the DOH collected and processed personal data of members of the public who had historically taken litigation against the Department.

3.3. The DPC issued a letter commencing the Inquiry (the ‘**Commencement Letter’**) by email and registered post to the DOH on 29 March 2021. The Commencement Letter notified the DOH that the DPC had commenced an Inquiry under and in accordance with section 110(1) of the 2018 Act.

3.4. The DPC commenced an own volition inquiry to independently investigate certain of the allegations. The inquiry focussed on 29 open litigation files. The cases had been brought by or

on behalf of individuals seeking access to SENs resources from the state. The DOH was named as a defendant in these cases. The Department of Education ('**DOE'**) was named as a co-defendant in many cases also. The Health Services Executive ('**HSE'**) is an agency under the remit of the DOH. It is the "service arm" of the DOH in relation to the services that are the subject matter of the SENs litigation. The Commencement Letter informed the DOH that the DPC was of the opinion that one or more provisions of the 2018 Act or the GDPR may have been contravened in relation to personal data in respect of which the DOH may be the controller. The Commencement Letter went on inform the DOH that the DPC considered it appropriate to inquire into the matter in order to establish a full set of facts so that it may assess whether or not the DOH had discharged its obligations as controller and determine whether or not any provision(s) GDPR and/or the Data Protection Acts 1988-2018 had been contravened by the DOH in that context.

3.5. The Commencement Letter set out that the opening phase of the Inquiry would include one or more physical inspections to be carried out by appointed authorised officers, whose powers are set out in section 130 of the 2018 Act. It also stated that during the Inquiry the DPC might require the DOH to respond in writing to requests for information and to provide all relevant documentation that informs those responses.

3.6. Four physical inspections were carried out for the purposes of this Inquiry by the Case Officers, acting as authorised officers of the DPC, at the head office of the DOH at Block 1, Miesian Plaza, 50-58 Lower Baggot Street, Dublin 2 between 1 April 2021 and 21 July 2021. The Case Officers conducted an interview (remotely) on 5 May 2021 with the Whistleblower.

3.7. The DPC proceeded to prepare an inquiry issues paper (the '**Inquiry Issues Paper**') to document the relevant facts established and the issues that fell for consideration by me as decision-maker for the purpose making a decision under section 111 of the 2018 Act in respect of this Inquiry. The Case Officers furnished the DOH with the Inquiry Issues Paper on 5 August 2021 and invited the DOH's submissions on any inaccuracies or incompleteness in the facts. In the Inquiry Issues Paper, the Case Officers isolated certain issues as warranting a determination on whether there had been an infringement of data protection law.

3.8. The Case Officers found that certain matters raised by the Whistleblower in the 5 May interview did not require further investigation from the point of view of determining whether there had been an infringement of the GDPR or the 2018 Act.[1] In relation to the Whistleblower's allegation that the DOH held a video of a child in a distressed state, the Case Officers examined an affidavit on the file and were satisfied that the video concerned was submitted as an exhibit to an affidavit by the plaintiff's own parent.[2] In relation to the open litigation files that the Case Officers inspected, they found evidence that the DOH had been sent information by the

[1] Inquiry Issues Paper, p19
[2] Inquiry Issues Paper, p12

Department of Education, but did not find evidence that the DOH proactively sought information about plaintiffs or their families from co-defendants other than the HSE.[3]

3.9. The Inquiry Issues Paper also identified practices in relation to which it determined it was necessary to consider whether there had been an infringement of the GDPR. In the context of seeking to resolve cases that had been filed against the DOH between 2000 and 2007, the DOH sought information from the HSE in 2017 and 2019 about the services being received by plaintiffs from the HSE, and also about the plaintiffs' and their families' level of satisfaction with services. This was done based on legal advice that there was a connection between current levels of service satisfaction and the chances of settling the case. In relation to allegations that the DOH sought information directly from doctors, the Case Officers found that in one of these cases the DOH engaged directly with a plaintiff's doctor in 2017 in the context of seeking an update from the HSE about the provision of services to that plaintiff and the plaintiff's satisfaction with services. The DOH maintains that this was an isolated incident, and that its aim was not to obtain clinical or confidential information. That plaintiff's case had been initiated in 2007, and while an appearance was filed that year, no further documents have been filed in the case since then.[4]

3.10. It was the DOH's policy not to inform data subjects about the collection of their personal data from the HSE. The HSE were specifically asked not to inform data subjects that the DOH had requested the collection of information.[5]

3.11. In relation to the Whistleblower's allegations about the DOH storing school reports, the Case Officers found school reports on some open litigation files. The DOH understood that it received those reports from co-defendants in the course of litigation, and did not proactively seek them from the Department of Education or other state bodies. The Case Officers also found evidence of those school reports being collected and processed more than a decade after the initiation of cases in order to determine whether an approach should be made to plaintiffs to settle cases.

3.12. The DOH provided submissions on the Inquiry Issues Paper on 4 October 2021. The submissions included some textual amendments and supplemental information relating to the facts as set out in the Inquiry Issues Paper in addition to legal submissions relating to the issues set out in the Inquiry Issues Paper. Those comments were analysed and the DPC amended the Inquiry Issues Paper accordingly. On 11 October 2021, the DPC finalised the Inquiry Issues Paper and sent it to the DOH.

[3] Inquiry Issues Paper, pp10-11, p18

[4] Based on High Court search results on 2 May 2023 for the case number provided by the DOH to the Case Officers.

[5] In the template used by the DOH to request personal data from the HSE in 2019 it says "This is *not* a request to contact any of the Plaintiffs involved in the litigation or their families or legal advisors and indeed we would request you not to do so in connection with this request."

3.13. Having reviewed the Inquiry Issues Paper and the evidence gathered by the Case Officers, I drafted my provisional views on whether there had been an infringement GDPR or 2018 Act. Those views were set out in the Draft Decision. On 9 March 2022, the DOH provided its submissions on that Draft Decision. Those submissions gave rise to some additional queries, which were circulated to the DOH on 11 August 2022. The DOH responded to those queries on 17 October 2022.

3.14. A Revised Draft Decision was subsequently provided to DOH on 3 May 2023. The DOH provided submissions on the Revised Draft Decision on 6 June 2023.

3.15. I am now obliged to consider all of the information obtained in the Inquiry and to reach conclusions as to whether I identify infringements of data protection legislation. In this Decision, I have taken on board the submissions received from the DOH on 9 March 2022, 17 October 2022 and 6 June 2023 and have set out my findings as to whether there has been an infringement of data protection law.

4. Scope of the Inquiry and the application GDPR

4.1. The scope of the Inquiry, which was set out in the Inquiry Commencement Letter, was to examine whether or not the DOH discharged its obligations in connection with the matters that had come to the attention of the DPC by the broadcast of *Prime Time* on RTE 1 on 25 March 2021 and to determine whether or not any provision(s) GDPR or the Data Protection Acts 1988-2018 had been contravened by the DOH in that context.

4.2. The Commencement Letter specified that the Inquiry would focus on Articles 5(1)(a), 5(1)(b), 5(1)(c), 5(2), 6, 9, 14, 24, 25, 30 and 35 GDPR. The Commencement Letter stated that the Inquiry might also focus on the areas of data protection governance and security of personal data.

4.3. In relation to the application GDPR, I am satisfied that the DOH fulfils the role of controller, as that term is defined in Article 4(7) GDPR, in circumstances where it determines the purposes and means of the processing of personal data held on its internal litigation files.

4.4. I am also satisfied that the processing falls within the material scope of the GDPR. Article 2(1) GDPR defines the Regulation's scope as follows:

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

4.5. Recital 15 GDPR provides guidance for interpreting the material scope of the GDPR:

> In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The

> protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

4.6. Article 4(1) GDPR defines 'personal data':

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

4.7. Article 4(6) GDPR defines 'filing system':

> 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

4.8. In this case, the data which was the subject of the Inquiry included information in filing systems and processed by automated means relating to identified and identifiable persons, such as plaintiffs who have commenced litigation against the DOH and their family members. Therefore, the data processed by the DOH falls within the definition of personal data under the GDPR, and the processing of that personal data by the DOH falls within the scope of the GDPR.

5. Issues for Determination

5.1. Following my review of the documents provided to me by the Case Officers, the DOH's submissions on the Inquiry Issues Paper, and the DOH's submissions on the Draft Decision and Revised Draft Decision, I have identified the issues that arise for determination.

5.2. The issues that I have identified for consideration in this Decision are as follows:

- **Issue A:** Whether, during the Temporal Scope, the DOH had a lawful basis under Articles 6 and 9 GDPR to process certain categories of personal data of data subjects on its SENs litigation files, and whether it complied with the principle of data minimisation in respect of this processing.
- **Issue B:** whether the DOH may legitimately rely on Article 23 GDPR and section 60(3)(a)(iv) or 162 of the 2018 Act to restrict the scope of the obligations of Article 14 GDPR to provide transparent information to data subjects in respect of SENs cases where personal information concerning data subjects is obtained from sources other than the data subjects.
- **Issue C:** Whether the DOH complied with its obligations under Articles 5(1)(f) and

32(1) GDPR in relation to the internal access to its litigation files.

5.3. I have also determined that the appropriate temporal scope for the consideration of Issues A and B is 25 May 2018 (the date of application GDPR) to 29 March 2021 (the date of the Commencement Letter) (the '**Temporal Scope**'). The temporal scope for Issue C is slightly shorter (25 May 2018 to 21 March 2021) for the reasons explained in my analysis of that issue.

6. Issue A: Whether, during the Temporal Scope, the DOH had a lawful basis under Articles 6 and 9 GDPR to process certain categories of personal data of data subjects on its SENs litigation files, and whether it complied with the principle of data minimisation in respect of this processing

6.1. This issue concerns whether the DOH had a lawful basis under the GDPR, during the Temporal Scope, to process certain categories of personal data of data subjects on its SENs litigation files.

6.2. In the Draft Decision, the matters addressed by this single issue spanned across five distinct issues. I note that in the DOH's submissions, it cross-referenced its submissions on other issues. There is also overlap between the issues, including the requirement for "necessity" as part of the data minimisation issue and as a component of the lawful bases upon which the DOH seek to rely. For ease, I have combined these into one issue in this document.

i. Relevant law

EU Law

6.3. Recitals 45 and 50 GDPR state

> (45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. … A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. …
>
> …
>
> (50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. … The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. …

> Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. …

6.4. Under Article 4 GDPR:

> For the purposes of this Regulation:
>
> …
>
> (2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
>
> …

6.5. Article 5 GDPR, entitled 'Principles relating to the processing of personal data', states, in paragraph 1 thereof:

> Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ("purpose limitation");
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
>
> …

6.6. Article 6 GDPR, entitled 'Lawfulness of processing', provides:

> 1. Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> …

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

…

(e) 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;

…

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall 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. … The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

…'

6.7. Article 9 GDPR, entitled 'processing of special categories of personal data,' provides:

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

…

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

…

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6.8. Article 23 of that regulation, entitled 'Restrictions', provides:

> 1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
>
> …
>
> (f) the protection of judicial independence and judicial proceedings;
>
> …
>
> (j) the enforcement of civil law claims.
>
> …

Irish law

Data Protection Act 2018

6.9. Section 38 of the 2018 Act entitled, 'Processing for a task carried out in the public interest or in the exercise of official authority' provides,

> (1) The processing of personal data shall be lawful to the extent that such processing is necessary and proportionate for—
>
> (a) the performance of a function of a controller conferred by or under an enactment or by the Constitution, or
>
> (b) the administration by or on behalf of a controller of any non-statutory scheme, programme or funds where the legal basis for such administration is a function of a controller conferred by or under an enactment or by the Constitution.

…

6.10. Section 41 of the 2018 Act entitled, 'Processing for a purpose other than purpose for which data collected,' provides,

> Without prejudice to the processing of personal data for a purpose other than the purpose for which the data has been collected which is lawful under the Data Protection Regulation, the processing of personal data and special categories of personal data for a purpose other than

the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—

(a) of preventing a threat to national security, defence or public security,

(b) of preventing, detecting, investigating or prosecuting criminal offences, or

(c) set out in paragraph (a) or (b) of section 47.

6.11. Section 42 of the 2018 Act entitled, 'Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes' provides,

(1) Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, personal data may be processed, in accordance with Article 89, for—

(a) archiving purposes in the public interest,

(b) scientific or historical research purposes, or

(c) statistical purposes.

(2) Processing of personal data for the purposes referred to in subsection (1) shall respect the principle of data minimisation.

(3) Where the purposes referred to in paragraph (a), (b) or (c) of subsection (1) can be fulfilled by processing which does not permit, or no longer permits, identification of data subjects, the processing of information for such purposes shall be fulfilled in that manner.

6.12. Section 45 of the 2018 Act entitled, 'Processing of special categories of personal data,' provides,

Subject to compliance with the Data Protection Regulation and any other relevant enactment or rule of law, the processing of special categories of personal data shall be lawful to the extent the processing is—

(a) authorised by section 41 and sections 46 to 54 , or

(b) otherwise authorised by Article 9.

6.13. Section 47 of the 2018 Act entitled, 'Processing of special categories of personal data for purposes of legal advice and legal proceedings' provides,

The processing of special categories of personal data shall be lawful where the processing—

(a) is necessary for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or

(b) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

6.14. Section 49 of the 2018 Act entitled, 'Processing of special categories of personal data for purposes of administration of justice and performance of functions,' provides

> Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where the processing respects the essence of the right to data protection and is necessary and proportionate for—
>
> (a) the administration of justice, or
>
> (b) the performance of a function conferred on a person by or under an enactment or by the Constitution.

Categories of personal data considered in this Decision

6.15. This section contains some further details on the type of information collected and processed by the DOH with which this Inquiry is specifically concerned. The DOH's submissions on the Draft Decision sought to apply all potential lawful bases to all categories of information it processed. Having considered those submissions, I determined that it was appropriate to reverse some of the findings of infringement in the Draft Decision in relation to some purposes for processing. It was necessary on this basis to restructure certain aspects of the analysis, and to categorise the personal data with which the inquiry is concerned and the purposes for which the DOH processed them, in order to assess whether the DOH had a lawful basis for this processing.

6.16. The Case Officers inspected the DOH's litigation files in the course of the Inquiry. These files contained documentation relating directly to litigation, including statements of claim and other documents filed with the courts, and legal advice relating to the proceedings in question. The files also contained the types of information outlined in Categories A and B outlined below. **The findings in this Decision relate solely to documents in Categories A and B, and makes no findings (of infringement or otherwise) in respect of any other information stored on the DOH's litigation files.**

Category A – Information collected from the HSE

- **HSE data requests:** The DOH sent information requests to the HSE seeking updates on plaintiffs. The full text of one of the template requests is set out in paragraph 6.71. The information request asked for details of the services being provided to plaintiffs, the levels of satisfaction that the plaintiffs and their families felt with services; and "*any other issues the HSE feels worth mentioning*." In addition to providing updates about the services being provided to plaintiffs, the responses from the HSE[6] in some cases included personal details of the plaintiffs and their families' circumstances, including: details of their living circumstances and jobs, whether their parents were having marital difficulties, whether the plaintiff was in a "*crisis*" and

[6] Each example relates to only one case.

services being received by plaintiff's siblings, the levels of contact between a plaintiff and their family, and in another case, information received directly from a plaintiff's doctor. The cases relating to these pieces of information were initiated in the following years respectively: 2007, 2002, 2007, 2005, 2004, 2007, 2001, and 2004. The updates related to three cases are undated, but were being retained throughout the Temporal Scope. The updates relating to the other six cases were sought in 2017 and 2019, and were retained during the Temporal Scope. In total, 24 out of the 29 case files examined by the Case Officers had been initiated more than a decade before the inspection. 21 updates were sought using the 2019 Template.[7]

- In another case, the DOH said, "*we don't want any clinical or confidential data*." In some cases, the HSE responded saying that the plaintiff was not known to it or that there were no service issues outstanding.

- The DOH explained that the sole purpose for which these updates were obtained was to determine what action should be taken in the case, i.e. to decide whether it was an appropriate time to seek to settle the case with the plaintiff. It said that in the absence of these updates, reaching out to the plaintiff could inappropriately reactivate the case.

- **Communication with a doctor:** In one case, the information request to the HSE led to the DOH communicating directly with a doctor who had seen the plaintiff as a patient. The doctor sent an update to the DOH of a consultation with the plaintiff, which included details about the plaintiff's medical condition and the treatments and medicine he was receiving. This information was received in 2017, before the date of application GDPR. It was retained by the DOH throughout the Temporal Scope. The purposes for retention during the Temporal Scope of the updates collected prior to the Temporal Scope evidently included seeking further updates for settlement purposes. In requests sent in 2019, the following line was included: "*We received the following update in … 2017.*[8] *If there has been no change please just confirm*." On 31 May 2018, a 2017 update was recirculated for the purposes of determining litigation strategy.

- **Transparency:** The DOH did not inform plaintiffs of any of these practices. When collecting information from the HSE it specifically asked that the plaintiff would not be informed about the information request. It relied on exemptions in the GDPR and 2018 Act in not informing plaintiffs about these information collection practices.

6.17. Documentation relating to the DOH's internal justifications for these practices was also provided to the Case Officers during the Inquiry, as follows:

[7] Issues Paper, [9]
[8] Ellipsis because different months were included in each email

- In 2017, the DOH received legal advice that it could collect and process personal data obtained from the HSE on the grounds of section 8(f) of the Data Protection Acts 1988 and 2003. This legal advice said that the DOH could process personal data for purposes relating to litigation. This advice did not refer to whether the processing would continue to be lawful under the GDPR.

- A 2021 Report to the Secretary General of the DOH stated that the DOH had been advised that, for GDPR purposes, it should confirm with the HSE whether there was any issue providing the information.

- The 2021 Report and other documentation provided to the DPC said that the information provided by the DOE was provided in the normal course of litigation for the purposes of the joint defence of litigation.

- The DOH was asked by the DPC supervision unit, "*Was any assessment made of the data protection impact of this processing, at the time that the processing commenced, or prior to the application GDPR on 25 May 2018? If so please provide details*."[9] The DOH replied, "*A data protection impact assessment has not been carried out in respect of the processing of personal data for the purposes of litigation.*"[10]

- The DOH also permitted the Case Officers to review the 29 SENs litigation files. On those files, there was documentation that explained the background to the processing from a litigation perspective. This documentation included a legal background approach summary that set out the rationale for its collection and processing of information from the HSE in high-level terms. This document explains that the DOH and other government departments decided to coordinate as co-defendants to adopt a well-managed approach to litigation. The Case Officers also reviewed correspondence between the DOH and its legal advisors that was sent in the course of specific litigation. Those documents discussed the different options available to the DOH at that stage of the litigation. Those options were discussed in relation to specific cases at specific points in time and included making contact with the plaintiffs to seek a settlement, seeking an order for striking out and continuing to let the case lie.

- A Senior Counsel report was provided to the DOH following the Whistleblower's allegations. That report did not draw any conclusions on the legality of processing by the DOH of information obtained from a HSE doctor for the purposes of data protection law. Indeed, the report recommended that the DOH confirm that it received legal advice following the exchange on whether the collection and processing of that information, and information obtained from the HSE more generally, complied with section 8(f) of the Data Protection Acts 1988 and 2003. The submissions received

[9] Email of 25 March 2021
[10] Letter from the DOH of 13 April 2021

from the DOH on 9 March 2022 noted that "*Receipt of said advice was confirmed by the Department*" but the DOH did not expand that point to make a further submission on compliance with section 8(f) of the Data Protection Acts 1988 and 2003.

- On 11 August 2022, I wrote to the DOH asking them to confirm whether it had further policy documentation relating to necessity or proportionality that had not previously been provided to the DPC. In response, by letter of 14 October 2022, the DOH said, "*The position of the Department on the necessity of collection of information has been explained fully in our Draft Decision Response. This is a policy position which was maintained by the Department throughout the Temporal Scope. The Department respectfully requests that the DPC engage with that position*."

Category B – Educational and health reports

6.18. The Case Officers found evidence of health and educational reports stored on the 29 litigation files. This information is summarised below. For the purposes of this Decision and the analysis below, I have separated this into (i) information that was received long after the litigation commenced, and (ii) information for which the date of circulation is unknown or which was received around the date of litigation.

i. **Educational reports received long after litigation was initiated:** The educational reports stored by the DOH were outlined in the Inquiry Issues Paper.[11] These were also summarised in a document from the DOH called "Action 1 Summary of educational reports." Information about the date of initiation of cases was contained in a document called "DOH – cases by service users' age." In relation to a case that commenced in 2004, the Case Officers found a report dated April 2008 by the National Education Psychological Service (NEPS) concerning a school-going child. A report of an educational psychologist prepared for NEPS in 2006 was stored on the same file, as was a report of a District Inspector of the Department of Education prepared in 2015 in relation to the child's education from primary school to third level. The Case Officers found no evidence that this information had been solicited by the DOH. There was a report on another file relating to litigation commenced in 2002 prepared by an educational psychologist in 2015 which is an assessment requested by the Department of Education, of the care plan prepared for the plaintiff by the provider. One email contained educational summaries from 2015 for six cases, five of which related to the 29 open cases examined. These were prepared by the Department of Education, summarising the special educational supports and services provided in each school year. Three of those cases were initiated in 2004, 2003 and 2007 and two were initiated in 2013. The cover email that was sent with these profiles said, "Subject to your advices we believe these cases should remain as they are, and we should "*let*

[11] Section 10 of the Inquiry Issues Paper

sleeping dogs lie."" The purpose of processing this information was outlined in response to the Inquiry Issues Paper as follows:

> Government Departments regularly adopt a joint strategy in defending litigation. It is normal practice for defendants to litigation to co-operate and share appropriate information with each other, required for obtaining legal advice and/or defending the proceedings, where they have a common interest in the issues and outcome of the proceedings.
>
> It is in the interests of all parties that a conclusion is reached. Both the Department of Health and the Department of Education are also very clear, regardless of litigation, that simultaneously, the primary duty of the HSE and the education system is to provide children and families with the required care and supports, in line with policy and legislation within existing resources. This policy intent to provide health and care supports is evidenced both through the level of resource and service delivery commitments in the HSE National Service Plans for disability services and specifically through the individual case HSE service updates.
>
> The Department is entitled to take the view that if information is copied to it by the CSSO or by its co-defendants that a determination has been made that it is appropriate and relevant to share that information, in relation to the anticipated, collective defence.
>
> Once the Department has received information in the context of litigation it becomes part of the litigation record and, as such, it is retained on the litigation file, subject to the same considerations discussed under Issues 1 and 2 above.[12]

ii. **Other educational and health reports:** The Case Officers also found summaries from 2014 on two files by local special educational needs officers relating to the provision of educational supports and services. Those cases had been initiated in 2013. In relation to a case commenced in 2017, the Case Officers found reports on one file relating to schooling that were included within the Book of Exhibits attached to an affidavit from the plaintiff's solicitors. There was a report on another file relating to litigation commenced in 2003 where psychologists working for Child Development Services provided a report as part of a letter of support addressed to the mother of the plaintiff. This was provided by the plaintiff's solicitors to the CSSO and forwarded by the CSSO to the Department of Health. It found a report from 2002 on one file relating to proceedings instituted in 2000 based on an assessment by an educational psychologist that had been prepared in response to the initiation of legal proceedings against the state, to provide an assessment of educational needs. Finally, there was one email relating to two cases attaching two excel files containing small number of rows of database extracts showing the July provision and home tuition applications. The email was sent in 2014, and the cases had been commenced in 2013.

[12] Submissions on Inquiry Issues Paper, p17

The DOH stored other health reports on its litigation files, and provided the Case Officers with details of all identified instances of where it stored such reports on its files, as set out in full in this paragraph. As outlined in the Inquiry Issues Paper, "During the third inspection, the Department of Health produced five manual files to the Case Officer (none of which have an electronic version). All of these files contain medical reports that were submitted to the Department of Health by the Midlands Health Board concerning plaintiffs in a particular geographical area. There is no evidence on the files to indicate that the reports were sought by the Department of Health and there is no understanding within the Department at this time of the reasoning behind the submitting of these reports to it. Nevertheless, five files contain medical reports submitted by the Midlands Health Board at a time unknown and these medical reports remain on the Department's SENs litigation files. This matter was discussed further at the fourth inspection at the Department of Health. Examples were given of two other cases, apart from the aforementioned five files, on which clinical reports are filed. The Department explained that clinical reports that were not solicited by it but which are held on file fall into two categories: (i) reports which the Department is aware of the source from which they were obtained (such as being submitted via family solicitors to the CSSO and then copied to the co-defendants); and (ii) clinical reports in respect of which the Department cannot definitively ascertain the chain of events that led to them being supplied to it (such as the five Midlands Health Board examples referred to above) but which the Department is satisfied that it has sufficient reason in the context of the ongoing litigation to retain the reports concerned on file."[13] In its submissions on 9 March 2022, the DOH clarified that it did not just provide the DPC with "examples of two other cases," but provided the DPC with all identified instances of cases in which it held clinical reports. There were only two other cases where the Department had not maintained on the paper files a full chain of documentary evidence demonstrating that all of the clinical reports for that case had been received in the context of litigation.[14]

The full text of that submission is as follows:

> The Department did not just provide "examples of two other cases". It provided the DPC with all identified instances, following reviews by external counsel, the SIU and Department officials, where there were clinical reports on litigation files. Review by external counsel further identified that of the many clinical reports relevant to these cases, there were only two other cases where the Department had not maintained on the paper files a full chain of documentary evidence demonstrating that all of the clinical reports for that case had been received in the context of the litigation.

The DOH's justification for retaining these reports is set out in its 4 October 2021 response to the Inquiry Issues Paper, as follows:

[13] Section 13 of Inquiry Issues Paper
[14] DOH's Submissions of 9 March 2022, [58]

these reports form part of the litigation record for these active cases and the Department is entitled to the presumption that the documents were provided to the Department on the basis that they would be relevant to and/or required for the defence of litigation. As such, the Department must retain the records in question, for the purpose of defending active litigation, and also in compliance with the National Archives Act 1986.[15]

Basis for processing in Irish law

6.19. The relevant law on which the DOH seek to base this processing are as follows:

- Sections 38, 41 and 47 of the 2018 Act, outlined in more detail above;
- National archiving legislation. The DOH's submissions from 9 March 2022 on this are set out below:

> [166] The National Archives Act 1986 and the National Archives Act, 1986 Regulations 1988 (S.I. No. 385 of 1988) are the primary legislative instruments applicable to the archival management of records of Government Departments.
>
> [167] A departmental record is defined in section 2(2) of the National Archives Act, 1986 and includes books, maps, plans, drawings, papers, files, photographs, films, microfilms and other micrographic records, sound recordings, pictorial records, magnetic tapes, magnetic discs, optical or video discs, other machine-readable records, other documentary or processed material made or received, and held in the course of its business, by a Department.
>
> [168] Correspondence received and sent for the ongoing management of SEN cases fall within the definition of "*departmental record*". As such, the application of the National Archives legislation fully applies to such records, including those that contain personal data as defined in Article 4 of GDPR or special categories of personal data as defined in Article 9. For records such as the "*clinical report*" referenced, which are subject to the National Archives Act 1986, the Department cannot lawfully dispose of them without the permission of the Director of the National Archives. This applies to the disposal of both paper and electronic records.
>
> [169] Section 7 of the 1986 Act sets out the required process for application by Government Department's for the disposal of departmental records. Subsection 4 is particularly relevant as it sets out the steps that must be met in order for a record to be disposed of. A key step in this process is that an officer of the Department has "*certified that particular Departmental records made, received or held by that Department and specified in the certificate, or a particular class or classes of such records so specified, are not required in connection with the administration of that Department*".

[15] Submissions on Issues Paper, 4 October 2021, p15

[170] For the reasons explained above, the steps outlined in section 7(4) of the National Archives Act 1986 have not been, nor can they be presently met, in the case of a report concerning active litigation. The Department must retain the record in question, and it cannot lawfully dispose of it in accordance with the National Archives Act 1986.

- Section 40C of the Health Act 2004, which provides,

  (1) The Minister may, where he or she considers it necessary in the public interest to do so for the performance of his or her functions (whether under this Act or otherwise), require the Executive to furnish him or her with such information or documents as he or she may specify that are in the Executive's procurement, possession or control, and the Executive shall do so within any period that the Minister may specify and, in any event, without delay.

- Various aspects of the rights and entitlements of litigants under Irish and EU law. Extracts from its submissions on these rights and entitlements from 9 March 2022 are set out below:

  [71] Litigants enjoys rights of the defence under EU law (see, e.g., Case C-418/11 *Texdata Softwares* EU:C:2013:588, §83), a right to fair proceedings under Article 47(2) of the Charter of Fundamental Rights of the EU ("**the Charter**"), the constitutional right to fair procedures and effective access to justice under the Constitution, and a right under Article 6 of the European Convention on Human Rights ("**the Convention**").

  [72] In particular, a central aspect of the right to fair proceedings under Article 47(2) of the Charter and Article 6 of the Convention is the right to equality of arms and procedural equality: see, e.g., Joined Cases C-514/07 P, C-528/07 P, C-532/07 P *API* EU:C:2010:541, §88; Case C-205/15 *Toma* EU:C:2016:499, §36; *Feldbrugge v the Netherlands* (App No 8562/79) 29 May 1986. In respect of Article 6, it is well-established that the ECtHR has held that each party must be afforded a reasonable opportunity to present their case, under conditions that do not place one party at a substantial disadvantage vis-à-vis the other party: Kress v France (App No 39594/98), 7 June 2001, §72; *Regner v Czech Republic* (App No 35289/11) 19 September 2017, § 146; *Dombo Beheer BV v the Netherlands* (App No 14448/88), 27 October 1993, § 33. In this regard, the Department also relies on Recital (4) to the GDPR, in light of which the relevant provisions GDPR should be interpreted and applied: "[*t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*".

  [73] To impose an obligation on a litigant such as the Department to review every document containing personal data such as arises from the DPC's analysis would unduly undermine the Department's defence of litigation.

…

[116] … once it is within its power, possession or procurement, the Department has a lawful obligation to retain all potentially relevant documentation -even in a dormant case, whether or not discovery has been agreed or ordered, and whether or not there are alternative means of proof. (See, *Orla McNulty v The Governor and Company of the Bank of Ireland t/a Bank of Ireland Group*, [2021] IECA 182.) The suggestion here and elsewhere (e.g. §10.39) that the Department would lawfully obtain a service update for the purpose of litigation, at a point in time (which the DPC accepts may be necessary), but then not retain it during the pendency of the litigation, is completely at odds with the ongoing duty of a litigant to retain relevant data. A Defendant would be rightly criticised if, having sought and obtained relevant documentation for the purpose of litigation and on foot of legal advice, it proceeded to destroy it. That being so, the criticism of the Department for "storing [information] indefinitely" (at §10.42) (i.e. during the pendency of ongoing litigation) is not well founded.

[117] There is a persistent suggestion that service updates might be necessary in "in some cases" or at particular points in time or in "revived litigation or settlement proceedings" only (e.g. §10.39), but not in dormant cases. However, the clear and uncontroverted evidence from the Department is that service updates were necessary "*in advance of any approach being made to plaintiffs to resolve the case*." Also, it bears noting that the obligation to progress cases falls on *both* parties to litigation.

[118] Here and elsewhere, there is an implicit misunderstanding as to the status of "*dormant*" cases. Litigation is either extant or not. The term "*dormant*" is a shorthand way of referring to a case in which there has been some hiatus or prolonged period of inactivity. However, that is not at all unusual in long running litigation, such as the SEN cases. Critically, however, dormant cases are not resolved or dismissed. They remain "*live*" proceedings, pending before the Courts. The parties' respective obligations and entitlements are not diluted in any way by the fact that the proceedings are dormant for a period of time. The notion that relevant documentation might be rendered irrelevant, unnecessary or disproportionate, by reason of a case being (temporarily) dormant is manifestly erroneous and irrational.

[119] The Draft Decision continually asserts that the Department may only process data that is "*indispensable to litigation*" and "*strictly necessary*." (§10.29). In the context of litigation, the assessment of what is necessary / indispensable / strictly necessary for litigation is generally based on legal advice (usually an '*advice on proofs*'). The Draft Decision underestimates the function of legal advice and the evidence from the Department that the information sought was on the basis of discussions with the Chief State Solicitor's Office and the Office of the Attorney General. Further, the Draft Decision fails to have due regard to the fact that the Senior Counsel Report found that "*the information shared between the parties is consistent with, and typical of, the sort of information which arises in such litigation*." Finally, the Draft Decision ignores the prior "experience and practice" of the

Department in settling litigation, mentioned in the Department's response to the Draft Issues Paper.

[120] Documentation may well be necessary and indispensable to litigation, even if the case is resolved prior to trial and even documents are never deployed in evidence. This was recognised by the Supreme Court in *Tobin v Minister for Defence* [2020] 1 IR 211. Although the following comments were made in the context of a contested discovery application, they apply *a fortiori* to the preservation of a party's own documentation (at 224, per Clarke C.J.):

> *"It is undoubtedly true that much discovered documentation does not find its way into the evidence. But it would be to underplay the potential importance of discovery to confine its contribution to ascertaining the true facts to the documents which ultimately find their way into the evidence. Discovery can also influence the evidence presented in other ways, such as by ensuring that it may be unnecessary to go into much documentary material, precisely because the party which has discovered the documents in question will almost inevitably have to present a case in oral evidence which is consistent with the documentary record. It would be a significant hostage to fortune for a party to present oral evidence which seemed inconsistent with documents which that party had itself produced on discovery, unless some compelling reason for the divergence could be given. It might turn out to be wholly unnecessary to refer to the documents in question in evidence but that would not mean that those documents may not have had a significant effect on the overall run of the case."*

The test for lawfulness

6.20. Elements of the test for lawfulness applicable to this issue were recently summarised by the CJEU[16] as follows:

> [29] … it must be pointed out that any processing of personal data, including processing carried out by public authorities such as courts, must satisfy the conditions of lawfulness set by Article 6 GDPR.
>
> [30] In that regard, it should be noted, first, that, according to Article 6(1)(e) GDPR, the processing of personal data is lawful if it 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.
>
> [31] In accordance with Article 6(3) GDPR, read in combination with recital 45 thereof, the basis for the processing referred to in Article 6(1)(e) of that regulation is to be defined by EU law or by Member State law to which the controller is subject. Moreover, the EU or Member State law must meet an objective of public interest and be proportionate to the legitimate aim pursued.

[16] Case C-268/21 *Norra Stockholm Bygg AB v Per Nycander AB,* Judgment of 2 March 2023

> [32] The combined provisions of Article 6(1)(e) GDPR and Article 6(3) thereof therefore require there to be a legal basis – national in particular – which serves as a basis for the processing of personal data by the relevant controllers acting in the performance of a task carried out in the public interest or in the exercise of official authority, such as those performed by courts acting in their judicial capacity.
>
> [33] Second, where the processing of personal data is carried out for a purpose other than that for which those data have been collected, it follows from Article 6(4) GDPR, read in the light of recital 50 thereof, that such processing is allowed provided that it is based, inter alia, on Member State law and that it constitutes a necessary and proportionate measure in a democratic society to safeguard one of the objectives referred to in Article 23(1) GDPR. As that recital indicates, in order to safeguard those important objectives of general public interest, the controller is thus allowed to further process the personal data irrespective of the compatibility of that processing with the purposes for which the personal data were initially collected.

6.21. For the special category data processed by the DOH, the processing was also required to be necessary for one of the purposes listed in Article 9(2) GDPR.

6.22. Further legal sources relating to each element of this test are set out below.

Clear precise and foreseeable

6.23. In *Schrems v Data Protection Commissioner* ('**Schrems I**') the CJEU commented on the need for a law permitting interference with rights under Article 7 and 8 of the Charter to be clear and precise:

> EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.[17]

6.24. In *SIA 'SS' v Valsts ieņēmumu dienests*, Advocate General Bobek indicated that if a legal basis lacks the requisite detail required by Article 8(2) of the CFR, an alternative means of clarifying the scope of the personal data to be processed is at an administrative level:

> In other words, the two regulatory layers, namely the legislative and the administrative, making up the eventual legal basis for the data processing, operate jointly. At least one of them must be sufficiently specific and tailored to a certain type or a certain amount of personal data requested. The more there is at the legislative, structural level for such data transfers, the less there needs to be in the individual administrative request. The legislative layer might even be so detailed and comprehensive that it will be completely self-contained and self-

[17] C-362/14, Judgment of 6 October 2015, [91]

executing. By contrast, the more generic and vague the legislative level, the more detail, including a clear statement of purpose which will thus delimit the scope, there will need to be at the level of the individual administrative request.[18]

Necessity

6.25. Necessity is an important concept in EU data protection law[19] with a specific meaning.[20] In several judgments, the CJEU has found that the processing of personal data, which is a limitation on the rights to privacy and personal data protection under Articles 7 and 8 of the Charter of Fundamental Rights of the EU ('**CFR**'),[21] must be strictly necessary for the purposes pursued.[22] Thus, the European Data Protection Board ('**EDPB**') has adopted guidelines stipulating that the strict necessity test precludes processing "*which is useful but not objectively necessary*."[23] Relevantly, this strict necessity test has been applied to personal data processed for the establishment, exercise or defence of legal claims in the *Rīgas* judgment.[24]

6.26. Strict necessity has several elements. The interference with data protection must be capable of achieving its stated objective.[25] CJEU case law also underscores that processing of personal data is not necessary if there are "realistic, less intrusive alternatives."[26] In that vein, there ought to be no equally effective available alternative manner of achieving the stated objective,[27] and any interference arising from the processing in question should be the least restrictive of the right.[28]

6.27. Additionally, the DOH cited two other descriptions of necessity from the case law of the CJEU in its submissions. In *Huber v Bundesrepublik Deutschland*[29] (which was cited in the Draft Decision) the CJEU held that the necessity of a centralised register could be demonstrated if

[18] Case C 175/20, Opinion of Advocate General Bobek of 2 September 2021, [82]
[19] European Data Protection Supervisor ("**EDPS**"), "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit," 11 April 2017 ('EDPS Toolkit on Necessity), which says that necessity "is an essential element with which any proposed measure that involves the processing of personal data must comply" at 2
[20] Case C-524/06 *Huber v Bundesrepublik Deutschland*¸ Judgment of 16 December 2008 ('Huber')
[21] EDPS quick-guide to necessity and proportionality (20-01-28_edps_quickguide_en.pdf (europa.eu)) accessed 30 November 2021 ('EDPS Quick Guide')
[22] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, ('Rigas'), Judgment of 4 May 2017, [30] (emphasis added)
[23] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019 ('EDPB Guidance on Article 6(1)(b)'), [25]
[24] Rigas (op. cit.), [29] and [30]
[25] Rigas (op. cit.), Opinion of Advocate General Bobek of 26 January 2017, [71]
[26] EDPB Guidance on Article 6(1)(b), [25], citing Rigas (op. cit.), [30] and Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, Judgment of 9 November 2010 ('Volker and Scheke')
[27] Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk*, Judgment of 20 May 2003, [88]
[28] In Volker and Scheke (op. cit) at [3], the CJEU held that it was "possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question..."
[29] Huber, (op. cit.)

(DOH's emphasis): "*it **contributes to the more effective application** of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals.*"[30] More specifically, that case related to an interpretation of the Data Protection Directive in light of the prohibition on any discrimination on grounds of nationality, and held that the requirement for necessity would be met in the context of putting in place a system for the registration of foreign nationals to implement legislation relating to the right of residence:

a) It contains only data which are necessary for the application by those authorities of that legislation; and

b) Its centralised nature enables that legislation to be more effectively applied as regards the right of residence of Union citizens who are not nationals of that Member State.[31]

6.28. Following (a) above, it is clear that the concept of necessity is closely linked to the data minimisation principle set out in Article 5(1)(c) GDPR. That principle requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

6.29. The CJEU has also held that the legislature was obliged to consider whether it was possible to envisage measures which will "*interfere less with the rights recognised by Articles 7 and 8 of the Charter **but will still contribute effectively to the objectives** of the European Union rules in question."*[32] This emphasises the "least intrusive alternative" aspect of the necessity test already highlighted but actually goes slightly further: in line with this decision an alternative measure that "contributes effectively" and is less intrusive with the rights to privacy and data protection should be chosen even if it is not "equally effective."

Proportionality

6.30. Proportionality is an assessment of the legitimacy of an aim, balanced against the scope, extent and intensity of the interference with a fundamental right.[33]

6.31. The concept of proportionality is closely related to the necessity test.[34] In Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB*, the CJEU considered the interference with fundamental rights caused by a particular processing activity before applying the necessity test. Due to the "seriousness of the interference with fundamental rights" that arose from the relevant processing activity in that case, the court found that only certain objectives pursued by

[30] Ibid, [62]
[31] *Huber,* [66]
[32] *Michael Schwarz v Stadt Bochum*, Case C-291/12, Judgment of 17 October 2013, [46]
[33] EDPS Guidelines on Proportionality (op. cit.), 10
[34] EDPS Toolkit on Necessity (op. cit.), 5

processing could justify that interference.[35] In essence, the severity of interference with rights was balanced against the importance of the objective pursued by the processing in question, with the court stating:

> since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data.[36]

6.32. Therefore, in certain cases where interference with rights is sufficiently serious, it can be appropriate to consider the manner in which a particular processing activity interferes with fundamental rights in tandem with the necessity test. Generally, however, proportionality will be considered after the necessity test has been applied.[37]

6.33. Whereas any processing of personal data amounts to an interference with the rights to personal data protection and private and family life under Articles 7 and 8 of the CFR,[38] the seriousness of that interference will depend on the context, and in that regard, the following factors are worth considering in the context of the processing by the DOH of information received from the HSE:

1. the scope of the processing, in terms of the number of people affected and whether it interferes with the privacy of persons other than the data subjects in question;
2. the extent of processing, including the amount of information collected and the period over which the data were collected;
3. the level of intrusiveness of the processing, taking into account the nature of the activity and whether it involves profiling or affects activities covered by duties of confidentiality, such as medical confidentiality;
4. whether the processing concerns vulnerable persons; and
5. whether it affects any other fundamental rights, such as the right to privacy.[39]

6.34. Relevantly in the context of this Inquiry, the EU court has discussed the proportionality between competing rights in the context of litigation.

6.35. In *Norra Stockholm Bygg AB v Per Nycander AB,* Judgment of 2 March 2023, the CJEU held,

---

[35] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis*, Judgment of 21 December 2016 ('Tele2 Sverige AB'), [102]
[36] Ibid, [115]
[37] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to the privacy and to the protection of personal data, 19 December 2019 ('EDPS Guidelines on Proportionality'), 10
[38] EDPS Quick Guide (op. cit.)
[39] EDPS Guidelines on Proportionality (op. cit.), 23-24

> [37] In those circumstances, the processing of personal data for a purpose other than that for which those data have been collected must not only be based on national law, such as the provisions of Chapter 38 of the RB, but also constitute a necessary and proportionate measure in a democratic society, within the meaning of Article 6(4) GDPR, and safeguard one of the objectives referred to in Article 23(1) GDPR.
>
> [38] Those objectives include, in accordance with Article 23(1)(f) of that regulation, 'the protection of judicial independence and judicial proceedings', which, as the European Commission noted in its written observations, must be understood as referring to the protection of the administration of justice from internal or external interference, but also to the proper administration of justice. Furthermore, according to Article 23(1)(j) thereof, the enforcement of civil law claims also constitutes an objective which may justify the processing of personal data for a purpose other than that for which they have been collected. It cannot therefore be ruled out that the processing of personal data of third parties in civil court proceedings may be based on such objectives.
>
> [39] However, it is for the referring court to ascertain whether the relevant provisions of Chapter 38 of the RB, first, meet one and/or other of those objectives and, second, are necessary and proportionate to the said objectives, so that they are capable of falling within the scope of cases of personal data processing regarded as lawful under the provisions of Article 6(3) and (4) GDPR, read in combination with Article 23(1)(f) and (j) thereof.

In the public interest and based on an objective of general public interest under Article 23(1) GDPR

6.36. As noted above, in *Norra Stockholm Bygg AB,* it was held that:

> [32] The combined provisions of Article 6(1)(e) GDPR and Article 6(3) thereof therefore require there to be a legal basis – national in particular – which serves as a basis for the processing of personal data by the relevant controllers acting in the performance of a task carried out in the public interest or in the exercise of official authority, such as those performed by courts acting in their judicial capacity.

6.37. This is reflected in section 38 of the 2018 Act, the full text of which is set out above. The provisions of Article 23(1) GDPR are set out above also.

Purposes for the processing

6.38. Based on a review of the submissions and the information collected during the Inquiry that there were two processing operations with two distinct purposes as follows:

- The processing of personal data received from the HSE or the DOE by *storage, internal circulation or other means* for the purposes of determining litigation strategy and whether it was an appropriate time to make contact with a plaintiff for settlement ('**Purpose A**');

- The *retention* of personal data for the purposes of complying with legal obligations or litigation requirements, such as legal hold or discovery obligations, or archiving legislation ('**Purpose B**').

6.39. Following the DOH's submissions, I have decided to reverse the findings of infringement in the Draft Decision relating to Purpose B as outlined in more detail below. First, I will consider the legality of processing for Purpose A.

6.40. Documentation in Categories A and B(i) were processed for Purpose A as part of a coordinated litigation strategy between the DOE and DOH.

6.41. The service updates sought from the HSE were for the primary or sole purposes of determining whether to settle a case. As noted in the DOH's submissions of 9 March 2022,

> [126.b] The Department's engagement with the HSE to receive updates on service provision flows directly from legal advice which clearly and directly indicated that in the absence of service updates, counsel would not be able to advise the Department on the case. As such, the Department operated at all times on the basis that the service updates were strictly necessary. The DPC has no basis for the assertion "legal advice about settlement discussions is not contingent upon the receipt of information about satisfaction with the services provided to plaintiffs". This is utterly and completely incorrect for these cases. The primary issue of contention in settlement discussions/mediation is satisfaction with services.
>
> [134.a] …the sole purpose of obtaining service updates from the HSE was to facilitate legal advice on action to take on litigation cases (i.e. to consider initiating settlement talks or engaging with the plaintiff to seek withdrawal of the claim).

6.42. The DOH claimed in a letter to the DPC of 10 October 2022 that "the Department did not receive information from the Department of Education for the purposes of managing litigation or determining whether it was an appropriate time to settle the case or for the purposes of determining the next steps in litigation and determining whether it was an appropriate time to settle the case."[40] This statement is contradicted by evidence collected in the Inquiry. An email from the DOE to the DOH in 2015 attached five educational profiles of plaintiffs and said, "Subject to your advises we believe these cases should remain as they are, and we should '*let sleeping dogs lie.*'" During the Temporal Scope, this email was retained on the files of cases in respect of which the DOH sought updates from the HSE in 2019 and for the purposes of determining whether it was an appropriate time to settle the case. A reference to this strategy is included in the spreadsheet relating to the CD case provided by the DOH to the DPC, which said, "It is the DES' opinion, as the Applicant/Plaintiff is now over 18 and given the passage of time since the case was instigated, that we should write to the Plaintiffs/Applicants requesting that they consider discontinuing proceedings on a back-to-back basis (i.e. both sides meet their own costs). This strategy is contingent upon there being no current service provision issues (from the health sector) for the Applicant/Plaintiff." The spreadsheet was last updated on 31

[40] At p3

July 2017, and was still being retained during the Temporal Scope of the Inquiry, during which time the DOH was continuing to seek updates from the HSE about the plaintiff using the Template.[41] The DOH referenced information sharing in the context of joint management of litigation with the DOE on multiple occasions in the course of the inquiry. For example, in an internal review document, the DOH said,

> In that context, it was agreed by the [Department of Education, the Department of Health], the AGO and the CSSO to develop, populate and regularly review and update an agreed template form for a subset of cases.
>
> In 2017, a revised case management template was agreed. This template was updated by the Department of Education, the Department of Health and the CSSO, respectively. It was considered that this template, with updated service information, would assist in identifying cases suitable for settlement as, in the absence of service updates, it would be difficult to advise on the settlement of those cases.[42]

ii. Analysis of Issue A

6.43. The elements of the lawfulness test outlined above will be applied to Purpose A and subsequently to Purpose B, to determine whether the DOH had a lawful basis to process Category A or B data under any of the national law/legislation on which it sought to justify this processing.

Purpose A

Clear, precise and foreseeable lawful basis; compatibility with earlier purpose

6.44. In line with Recital 41 and Article 6(3) GDPR, the legislative basis underpinning Article 6(1)(e) must be clear and precise and its application must be foreseeable. Processing of re-purposed personal data under Article 6(4) GDPR must be compatible with the original purpose of collection, having regard to the factors set out at Article 6(4)(a)-(e). As the concepts of foreseeability and compatibility are similar, I will take these analyses together for structural purposes.

6.45. At 10.17 of the Draft Decision, I found that the DOH had, in principle, a lawful basis to process personal data for legal advice and litigation. In its submissions of 9 March, the DOH emphasised this sentence of the Draft Decision, stating,

> On the fundamental issue of lawful basis, the Draft Decision fairly acknowledges that *there is a lawful basis* for the processing of personal data by the Department as described in Issue 3 as follows: "*the*

[41] Email from DOH to HSE on 16/07/2019 at 11:52
[42] p12

[Department of Health] ***has a legal basis****, in principle, to collect and process personal data for the defence of litigation or in order to seek legal advice."* (Draft Decision at 10.17, emphasis added.) [43]

6.46. It must be emphasised, in response, that the Draft Decision did not determine that the DOH had a clear, precise and foreseeable lawful basis to process personal data **for the purposes of determining an appropriate time to settle a case** (Purpose A). That question was not considered further, as it was determined that the DOH had no lawful basis to process personal data on grounds of necessity or proportionality. For completeness, and to respond to the DOH's submissions, I have included more detail on this issue here.

6.47. The plain text of the legislation relied upon by the DOH to process personal data for Purpose A does not make it clear, precise and foreseeable that personal data would be collected or processed for the purposes of seeking to determine an appropriate time to settle a case. Retaining or processing files for archiving purposes is unrelated to processing for the purposes of litigation, let alone for the purposes of settlement. The National Archives legislation sought to be relied upon by the DOH thus does not make it clear, precise or foreseeable that processing will be carried out for Purpose A.

6.48. There is no specific reference to processing for the purposes of legal claims or advice in the Health Act 2004, or the provisions of the 2018 Act relating to processing for the purposes of statutory functions. These provisions permit processing that is necessary to carry out the DOH's functions. "Functions" is defined in the Interpretation Act 2005 as including "powers and duties."[44] As a state department, the DOH has a common law power to sue and be sued. Defending legal claims and litigation is thus a function of the DOH, and processing for this purpose could be based on the Health Act 2004 or section 38 of the 2018 Act. The 2018 Act also, separately, permits processing of personal data for the purposes of legal advice, legal claims or litigation in sections 41 and 47.

6.49. None of the provisions of the Health Act 2004 or of the 2018 Act clearly state that litigants can collect information for the sole purpose of determining whether it is an appropriate time to settle a case. However, the broad references in the 2018 Act to "legal claims" and litigation are generalised enough to capture processing for the purposes of settlement – this is an intrinsic aspect of litigation.[45] Moreover, at common law and under the 2018 Act, litigants have a number of rights and entitlements relating to litigation. These are not set out in a clear code of law, given the nature of Irish law, which can be derived from the constitution and from precedent. In the context of litigation and legal advice, it would not be possible for legislation to be prescriptive about the personal data that would need to be processed in any given situation. The categories of personal data that will need to be processed will be determined by the relevant context of the legal advice sought or the litigation in question.

[43] At paragraph 76
[44] Interpretation Act 2005, Sch1, pt2
[45] DOH's Submissions of 9 March 2022, [243.f]

6.50. Therefore, while the legislation sought to be relied upon by the DOH does not clearly and precisely reference settlement of claims, I do not consider this determinative of the question of whether there is lawful basis to process personal data for Purpose A in the context of the Irish legal system in a general sense.

6.51. Turning to foreseeability, the final limb of the test, I consider that there would be a general awareness among members of the public that if they take litigation related to state services that the relevant department(s) would process personal data about the services received. This includes information sought from the HSE in response to question 1-2 of the Template and information of the type set out in Category B.

6.52. However, I do not consider it foreseeable that the remainder of information in Category A be processed for Purpose A based on these common law entitlements or the provisions of the 2018 Act. In particular, the processing is not foreseeable in the following specific circumstances:

- A case was initiated on the plaintiff's behalf when they were a child;
- The personal data was collected and processed more than a decade after their case was initiated; and
- The personal data included details of their private lives that did not relate to the substance of litigation.

6.53. Although this processing relates to litigation in a broad sense, it does not relate directly to any of the rights and entitlements of litigants relied upon by the DOH. It does not relate directly to the achievement of a settlement. It relates solely to the timing of a settlement, and to the strategy surrounding extant litigation. The information was collected in the context of a different purpose – the provision of state services to individuals who also happened to be plaintiffs in litigation. It would not be reasonably expected that this type of private information would be repurposed for litigation. Therefore, I do not consider that any of the lawful bases sought to be relied on by the DOH had a foreseeable application to Purpose A.

6.54. Therefore, in the specific circumstances of a state body collecting and otherwise processing personal data sought from the HSE in response to question 3-4 of the Template for Purpose A, I do not consider that there is a clear, precise and foreseeable lawful basis for this processing under Irish law.

6.55. For completeness, I will now also consider whether the processing was compatible with the original purpose for which the personal data were collected.

6.56. The HSE came into possession of information received in response to question 3-4 of the Template, which related to the private lives of plaintiffs and their families, through the provision of state services. There was no link between this purpose and the purpose of litigation, as

required by Article 6(4)(a). The information was collected in the context of a relationship between a state body providing services to vulnerable individuals, which is a relevant consideration for compatibility under Article 6(4)(b). The personal data included special categories of personal data, which is relevant to consider under Article 6(4)(c). Under Article 6(4)(d), I consider that the consequences of the processing for data subjects could result in a lower financial pay out to them. The personal data was not encrypted or pseudonymised – a relevant consideration under Article 6(4)(e) – but stored in plain text in the DOH's electronic and paper files.

6.57. For all of these reasons, I do not consider the repurposing by the DOH of information originally acquired by the HSE about the private lives of plaintiffs and their families received in response to questions 3 and 4 of the Templates to be compatible with the original purpose under Article 6(4) GDPR. While I note that section 41 of the 2018 Act permits the re-purposing of personal data where it is "necessary and proportionate" for the purposes of legal advice, claims and proceedings, Article 6(4) GDPR takes supremacy over Irish law, and the compatibility test must apply equally when controllers seek to rely on section 41. The analysis of necessity and proportionality below also applies equally to the application of section 41 of the 2018 Act.

Conclusion: I do not find that the DOH had a clear, precise and foreseeable lawful basis to process personal data about the private lives of plaintiffs and their families sought from the HSE in response to question 3-4 of the Template for Purpose A, as required by Article 6(1)(e) GDPR. I also do not find that the processing personal data sought from the HSE in response to question 3-4 of the Template for Purpose A complied with the requirements of Article 6(4) GDPR that processing for a purpose other than that for which the personal data have been collected be compatible with the original purpose for collection.

Necessity

6.58. The DOH argues that it was necessary to collect information from the HSE for the purposes of determining an appropriate time to settle the case. Necessity is a pre-condition to reliance on various provisions sought to be relied upon by the DOH. As noted above, processing based on section 41 of the 2018 Act has a requirement of necessity and proportionality. This is also a pre-condition for reliance on section 38(1) of the 2018 Act. In order to process based on Article 6(1)(e) GDPR, the processing must have been necessary for a function of the DOH. For the special category data in Categories A and B, processing must have been necessary for the "establishment, exercise or defence of legal claims" under Article 9(2)(f) GDPR. Processing under Purpose A was not carried out for archiving purposes, so I do not consider archiving legislation or Article 9(2)(j) GDPR[46] to be relevant to the necessity test.

[46] This provision permits processing of special categories of data where "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

6.59. The DOH said its engagement with the HSE to receive updates on service provision "*flows directly from legal advice which clearly and directly indicated that in the absence of service updates, counsel would not be able to advise the Department on the case. As such, the Department operated at all times on the basis that the service updates were* strictly necessary."[47]

6.60. The DOH also said,

> In consultation with the Chief State Solicitor's Office, the Office of the Attorney General and its State co-defendants, the Department of Health accepted, based on legal advice, that it is necessary for the resolution of these cases that updates would be sought on the services being provided to plaintiffs, to determine the level of satisfaction with those service in advance of any approach being made to plaintiffs to resolve the case. The relationship between the successful resolution of cases and satisfaction with services, which are the subject of the claims against the State defendants, including the Department, has been established through experience and practice.[48]

6.61. Above, in the examination of whether the DOH had a clear, precise and foreseeable lawful basis I considered the various legal provisions upon which the DOH has sought to rely. That analysis highlighted that, whichever provision sought to be relied upon by the DOH under the 2018 Act or the Health Act 2004, the processing must have been necessary for the purposes of legal claims or litigation. To recap, in respect of their statutory powers and functions, administrative bodies have a common law power to sue and be sued under Irish law.[49] The Health Act 2004, common law rights of litigants and the 2018 Act each set out processing grounds relating to legislative functions, litigation and legal advice. Therefore, although the DOH seeks to rely on the Health Act 2004 and section 38 of the 2018 Act in addition to the provisions of the 2018 Act specifically relating to legal advice or litigation, the relevant "functions" of the DOH in the context of Purpose A are its functions as a state defendant. Processing for Purpose A must therefore be necessary for legal advice or litigation, whether the DOH relies on section 38 of the 2018 Act, the Health Act 2004, or the sections that specifically reference legal advice and litigation.

[47] DOH's Submissions of 9 March 2022, [126]

[48] DOH's Submissions of 4 October 2021, page 15

[49] Section 2(1) of the Ministers and Secretaries Act 1924 states that "Each of the Ministers, heads of the respective Departments of State mentioned in section 1 of this Act… may sue and (subject to the fiat of the Attorney-General having been in each case first granted) be sued under his style or name aforesaid." In *McCauley v Minister for Posts and Telegraphs* [1966] 1 IR 345, s.2(1) was held to be "repugnant to the Constitution in so far as it requires the fiat of the Attorney General to be obtained before proceedings in the High Court can be validly instituted against a Minister for State." In line with the principle of severance set out in Article 15.4 of the Constitution (see Doyle, O *Constitutional Law: Text, Cases and Materials* (Clarus Press, 2008), the remainder of the provision remains valid. In relation to the existence of the power to sue and be sued, see also Hogan, G, Morgan, DG and Daly, P, *Administrative Law in Ireland*, (5th ed, Round Hall, 2019), [10.36].

6.62. Moreover, the purposes for which the DOH claimed the processing were "necessary" all related to legal claims and legal advice. It has not argued that there are any other functions for which the processing is necessary. The analysis in this section will therefore focus on an examination of whether the processing was necessary for the purposes of legal advice, claims or proceedings by reference to the following aspects of the necessity test:

- The use of the minimum data necessary for the relevant purpose;
- Whether the processing is capable of achieving the stated objective;
- Whether there are equally effective alternatives available less intrusive to data subject rights;
- Whether there are alternatives available that still contribute effectively to the stated aim.

Minimum data necessary for the purpose

6.63. The concept of necessity is closely linked to the data minimisation principle set out in Article 5(1)(c) GDPR. That principle requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." In that regard, the DOH did not have clearly defined parameters for the information that it sought to collect. It sent an information request to the HSE with four questions. The first two related to current and future plans for therapeutic provision. The third related to family satisfaction with services. The fourth was a request for "any further information worth mentioning" and yielded responses that related to a plaintiff's private life, as outlined in more detail above. It is unclear, by reference to the questions in this request, what the DOH considered "necessary." The responses to the third and fourth questions were broadly at the discretion of the HSE. The nature of the information that was specifically considered "necessary" is therefore unclear.

6.64. The DOH sought to draw a distinction between one event in 2017 when personal data were obtained from a doctor directly and the other situations in which it sought updates from the HSE. When its template information request was sent to the HSE in this particular situation, it was subsequently circulated to a HSE doctor. The doctor saw the plaintiff as a patient after the information request had been received and provided an update to the DOH following that medical consultation. The update included details of the family circumstances of that plaintiff as well as medical information that had been obtained from the patient.

6.65. The following summary of this email exchange was set out in the Draft Decision:

> 7.3. The branch of the HSE to which the email was circulated responded to the DOH providing a general update in relation to the plaintiff's current living and schooling circumstances, including details of difficulties in the plaintiff's family circumstances. That reply was copied to a manager in another division of the HSE that also provided services to the plaintiff. The DOH acknowledged receipt of the first response and requested that the manager who was copied provide an update with regard to the individual's situation as regards the additional services.

> 7.4. Then, a HSE hospital doctor sent an email to the DOH stating that they had been asked by their managers to provide clinical information about a patient. The doctor asked whether the patient and their parents were aware of the request and whether consent to release details had been given. The DOH responded to the doctor confirming that it had not contacted the individual or their parents. It further requested that no contact be made with the individual or their family on the matter as such contact could have adverse implications for the defence of the legal proceedings. The DOH's email also outlined that "a significant reason for our request to HSE for an update on services received/planned and the family's degree of satisfaction/dissatisfaction with same, is to help us decide whether it may be advisable – or not – to initiate such contact against the backdrop of long-dormant legal proceedings." It went on to include some details of the plaintiff's case against the state. The reply from the DOH stated that the position on consent and consultation would be double-checked with the DOH's legal advisers and that the Department would revert to clarify as soon as possible.
>
> 7.5. The doctor replied to the DOH stating that they were due to see the plaintiff as a patient the following day and that they were not aware of a complaint or outstanding legal issues in the case. The DOH replied to the doctor stating, among other things that it was happy to withdraw its request for information "for the moment and revert in about a year's time, assuming nothing further happens to progress the case in the meantime." The following day, the doctor sent an email to the DOH in relation to the plaintiff. Within that email the doctor provided an update about the plaintiff that included certain clinical information about the plaintiff's medical condition and meets the definition of "data concerning health" in Article 4(15) GDPR. The DOH replied, thanking the doctor for their email and stating that it would revert sometime the following year to request another update.

6.66. This scenario was distinguished by the DOH in an internal review that followed the public allegations by the Whistleblower. In those allegations, the Whistleblower claimed that the DOH obtained updates directly from doctors. The DOH found that this was the only situation in its 29 open litigation files whereby information was obtained directly from a doctor. It sought to distinguish this from its general practices regarding information collection from the HSE, saying that the direct engagement with a doctor was inadvertent and that it had no experience of a doctor replying to them directly in relation to any other information request.

6.67. In its submissions on the Draft Decision, the DOH said,

> [46] it is correct to state that the receipt of the information was inadvertent. There is no evidence to suggest that the Department had ever received this extent of information in response to a service update, or had on any other occasion received a service update directly from a clinician. The Department sought a service update. It did not seek a clinical report or clinical information, nor did it intend to seek such information. There is no evidence to suggest that the Department was intentionally seeking clinical information. There is no evidence to suggest that the Department had sought anything other than the type of information usually provided.

6.68. It needs to be emphasised that the Inquiry was established to investigate whether there were infringements of data protection law arising from the allegations. For the purposes of data

protection law, the definition of "data concerning health" is broader than just clinical information or information that is subject to medical confidentiality. It includes any "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[50] Therefore, from a data protection perspective, the distinction between the situation where there was direct engagement with a doctor and the other situations is less pronounced. All of the information requests sought health data, which is a special category of personal data under the GDPR. Whether the engagement with a doctor was "inadvertent" or not, there was a clear intention to obtain special category data on the face of the request.

6.69. However, I do find that the situation where there was direct engagement with a doctor is a more serious interference with data subject rights, as there is a legal duty of confidence specifically arising from that relationship, and a reasonable expectation that any information obtained will be held and used in confidence. I have taken this into consideration in relation to the exercise of corrective powers.

6.70. More generally, the DOH's submissions on this particular incident highlight the underlying lack of necessity driving its approach. The DOH has made contradictory statements about this information. Its internal review said that the information collected from a doctor should be returned and not held on file.[51] The DOH subsequently said that the information should have been redacted.[52] It also said that it needed to continue to process the personal data for litigation purposes.[53]

6.71. The DOH submitted that the Draft Decision took too broad a view of the information request in drawing a conclusion that it was "inevitable" that medical information would be received in one specific case.[54] The DOH submitted that it only requested a "*brief service update*" and that the request should be viewed in that context. It also submitted that the "parameters of this request are intended to fall within the management of the litigation case and the service update."[55] In its submissions of 9 March 2022, the DOH said,

> 131. As already explained above, the wording included in the requests to the HSE must be seen in the context of the request being made. The wording, as the Department understands it, is a request for the HSE to communicate any other issues the HSE feels worth mentioning in the context of the service update request and the litigation case. It is very clear from the template letter, quoted by the DPC, that the parameters of this request are intended to fall within the management of the litigation case and the service update – the request clearly states (emphasis added): *This query relates to one of a number of historic litigation cases taken*

[50] GDPR, Article 4(15)
[51] Internal Review, p20
[52] DOH's Submissions of 9 March 2022, [49]
[53] Ibid
[54] Ibid, [22]
[55] Ibid, [30]

against the HSE [and] this Department…which have been dormant in the High Court for some time. In considering how best to manage these cases, we require, at the request of our legal team, a brief service update from HSE on the above individual under the headings listed 1-4 below please. The update should please either confirm no change to the details provided at the last update (see below) or include a brief up-to-date description of

1. Current service provision if any provided by/via the HSE

2. Plans, if any for future health related/therapeutic service provision,

3. Most recently reported levels of family satisfaction or otherwise with service provision/service plans or generally

4. Any other issues HSE feels worth mentioning

6.72. On the other hand, the DOH has effectively conceded that the requests were too broad, by saying that the "it is accepted that the wording of question 4 might be amended."[56]

6.73. Moreover, the only detail of the litigation that was provided to the recipients of the request was identifying information about the plaintiff. The request was not framed by reference to any specific facts or circumstances that would allow the recipient to provide specific relevant details. The DOH submits that it was not even possible to include those details without breaking privilege. It said that it would be inappropriate to set out "a more detailed rationale behind privileged legal advice that the information was required. Further detail would have resulted in a vitiation of the Department's legal privilege for that advice, and so could not be contemplated."[57] In that way, the DOH concedes that it was not possible to include further details in the request that would have reduced the risk of receiving excessive information.

6.74. The inclusion of this broad catch-all question was therefore an approach that risked receiving excessive information. In practice, the information received was detailed and sensitive. The Templates resulted in the circulation of information relating to plaintiff's private family and life circumstances including those outlined in paragraph 6.16 above. Although the DOH concedes that it could amend the last question of the request, which would result in less information being circulated, it also, in practice, used some of the sensitive information obtained to formulate its litigation strategy,[58] and continued to engage in these practices following the entry into force GDPR, risking the collection of equally sensitive information. The fact that the DOH says that it could amend the final question despite the fact that it used this type of information for its strategy contradicts whether it can consider the overall approach to be "necessary." The omission of this question would result in the omission of information that the DOH actually used to formulate strategy. If it could omit this question, and pursue a strategy that did not result in

[56] Ibid, [234]
[57] March Submissions, [42]
[58] See for example email from 31/05/2018

this type of information being collected, then it is unclear how the DOH can be convinced that its entire strategy was "necessary" at all.

6.75. As a result of these confused and contradictory statements, it is clear that the DOH had no policy position in relation to the amount of information that it was necessary to retain and process during the Temporal Scope. Particularly in the context of sensitive, special category data, this approach is inappropriate. It was incumbent upon the DOH to have had a clear policy in place throughout the Temporal Scope about the amount of information that it needed to collect for its purposes.

6.76. The DOH also stated in earlier submissions that it can, in the course of its work, "request information and then make a judgement about how it uses the information it receives."[59] That approach creates serious risks for the rights of privacy and data protection, and the DOH should take steps to ensure that it does not collect excessive information, particularly in light of its broader obligations relating to archiving. The subsequent justification of storage does not legitimise the initial collection or continued use for the purposes of determining appropriate times to settle litigation.

Capable of achieving the stated objective

6.77. Secondly, the necessity of the use that was made of this information is also doubtful. The cases in question had been "dormant" for up to a decade, and the DOH intentionally let certain cases lie where it had not determined that it was an "appropriate" time to seek a settlement. There was therefore no perceived imperative to settle the cases. This calls into question the DOH's arguments as to why the information collection was necessary. The only reason it claimed the information was necessary was to seek a settlement. In circumstances where the cases had been dormant for over a decade and where the DOH was intentionally letting the case lie, they were bearing the risk of reactivation by the plaintiff at all times. The arguments as to necessity imply that there was a financial risk to the state in probing the cases at the wrong time – however, this implies a false binary – the DOH did not perceive a need to probe the cases at all. The financial risk only arose at the point of seeking a settlement or reactivation – if, to use the DOH's language – the "dog" was woken at the wrong time, the case could be reactivated, increasing the financial cost to the state.

6.78. In fact, the strategy goes against the state's obligation to keep the case moving through the courts. The DOH itself mentioned this obligation.[60] In *AIB v Boyle* ([2020] IEHC 377) the court said,

> Whilst there can be no doubt but that the moving party has the greater obligation of expedition overall, nonetheless the defendant's interaction or lack of it, as the case may be, with the delay of which he later complains, whether active or purely inactive, to use such phrase, may rightfully attract

[59] Submissions on Inquiry Issues Paper, p8
[60] DOH's Submissions of 9 March 2023, [117]

> condemnation by virtue of many other circumstances such as: the identity and character of the particular defendant; the position which he holds; whether that be public or private; the standing and accountability of that position, whether it be representative of the public, of an institution which it serves or otherwise; and the nature of the issues which he is called upon to answer.

6.79. The DOH's strategy of avoiding reactivation appears to go against its the duty to keep the case moving through the courts. It benefited the DOH that the details of the case were not probed by the Court. It also benefited the DOH if it settled at the right time, thus dispensing of the risk of a significant order for damages in relation to its obligation to ensure the provision of services to plaintiffs.

Equally effective alternatives

6.80. The necessity test requires a consideration of whether there are alternative means available that are less intrusive to data subject rights.

6.81. In that vein, there are alternative means of handling litigation that are less intrusive to data subject rights. The information collected did not relate to the substance of litigation or the DOH's defence. Legal advice about settlement discussions is not contingent upon the receipt of information about satisfaction with the services provided to plaintiffs, and can be provided without obtaining that specific information. In relation to the DOH's submission that it received legal advice that the information would assist with settlement, it should be borne in mind that Articles 6(1)(e) or 9(2)(f), as implemented by the 2018 Act, do not permit processing on the basis of legal advice; they permit processing only where it is necessary to receive the legal advice. The processing was also not for the purpose of putting in place a litigation hold. I do not consider that processing for Purpose A was justified by those rights and entitlements of litigants.

6.82. In its submissions of 9 March 2022, the DOH said,

> 126.d … At § 10.41 of the Draft Decision, where the DPC states that the GDPR and 2018 Act, do not permit processing on the basis of legal advice; they permit processing only where it is necessary to receive the legal advice. With respect, this distinction is not applicable to the present situation. The clear evidence is that this information was sought on foot of legal advice and was necessary to receive the legal advice concerning settlement. In any event, section 47 of the 2018 Act refers to "processing— [being] (a) is necessary for the purposes of providing or obtaining legal advice," which it was here.

6.83. The involvement of lawyers or the litigation context does not make the processing "necessary" for use in that legal or litigation context. In fact, a finding that any processing of personal data on the basis of advice from lawyers or in relation to litigation is lawful would create risks for data subjects – the involvement of lawyers in discussions on a certain topic cannot be used to render processing lawful that would otherwise not be. That is why it is important to consider whether the proposed processing is genuinely necessary for legal reasons that fall within the listed categories in section 47.

6.84. To the extent that the processing was necessary, it was for a very narrow purpose: to collect as much information as possible to inform a strategy to settle a case that the DOH would have otherwise "let lie" at a time that had the maximum financial benefit to the state. This appears to be the DOH's interpretation of its competing obligation as a litigant to keep the case moving as against the obligation to ensure minimum public expenditure as a state body.

Whether there are alternatives available that still contribute effectively to the stated aim

6.85. Noting the *Schwarz* case cited by the DOH, there is a requirement to consider measures that will interfere less with rights, and still contribute **effectively** to the aims pursued. Even if it were accepted that processing for Purpose A was necessary to minimise state expenditure on litigation, it must be considered whether there are other **effective** ways for the state to manage litigation that interfere less with data subject rights.

6.86. By comparison with the DOH's practices, there are alternative means of handling litigation that do not involve the collection of this type of information. In many cases, defendants will not have all of the resources of the state at their disposal to "hunt down" or "chase up" various agencies, civil servants or even medical professionals for details of the current mind-set of plaintiffs towards certain services. That does not mean that its "equality of arms" as litigants is at stake, as implied by the DOH at paragraph 72 of its submissions of 9 March 2022. It means it has to make a choice about the next steps in the case without intruding into the private lives of citizens who have historically initiated litigation. All of the relevant options remain open to someone in that position: DOH can seek to settle the case, let it lie, or seek an order to have it struck out. The DOH rights and entitlements as a litigant before the courts would not be affected at all if it did not have information to make predictions about the mind-set of plaintiffs. These approaches would have interfered much less with data subject rights, and would still have contributed effectively to the aims in question. They also are the only approaches available to the majority of litigants who do not have the resources of the state to find out information about litigants of the nature that the DOH sought.

Conclusion on necessity: Based on the analysis above, according the DOH, processing for Purpose A was necessary for the specific purpose of seeking to minimise state expenditure on litigation. However, due to the broad and scoping nature of its requests sent to the HSE, I do not consider that the DOH sought to ensure that it collected the minimum amount of personal data necessary for this aim. I also consider that there were alternative means of handling litigation that would still contribute effectively to the aims pursued by the DOH. Therefore, I do not consider that all of the DOH's processing of personal data for Purpose A was "strictly necessary" for the aims it pursued.

Proportionality

6.87. Above, it was considered that the aim for which the processing may have been necessary was to minimise state expenditure on litigation. The strict necessity of this aim was called into question by the fact that there were alternative ways for the state to manage litigation effectively, leading to the conclusion that the processing was not strictly necessary. Even where

processing is necessary for certain purposes, a proportionality test must be applied to determine whether it is lawful. For completeness, I will consider proportionality here.

6.88. The DOH said that the Draft Decision had engaged in a flawed proportionality assessment by failing to consider the DOH's obligations and entitlements as a litigant before the courts. The DOH said that it was proportionate for it to have processed personal data for the purposes it did because the plaintiffs had put the services and service satisfaction at issue by taking the cases.[61] Its explanation of why the processing was proportionate included only reasons in favour of the processing from its perspective, and there is no evidence that it engaged in any form of balancing assessment to consider the impact of the processing on data protection. The DOH included various details of its own rights and entitlements as a litigant before the courts, including its obligation to put in place litigation holds to prevent the destruction of relevant documents. This obligation does not relate to Purpose A. The assessment of proportionality and necessity under the GDPR must relate to the purposes for which the documentation was actually collected and received. It is hypothetical, therefore, to say that exactly the same information would have been lawfully collected if it was collected for other purposes. Whether the DOH had a separate obligation to store the information once it had been generated is also beside the point in considering the validity of processing that personal data for Purpose A. Where there is an obligation to store certain personal data, it should be stored for those purposes only and not further processed for unconnected purposes.

6.89. In its submissions on the Draft Decision, the DOH referenced a number of rights and entitlements of litigants that it argued would permit it to process personal data in the way that it did. Those rights and entitlements ranged from the preparation of a defence, putting a litigation hold in place and ensuring equality of arms. However, those rights and entitlements are unrelated to the real purpose for which the DOH sought information from the HSE, which was to seek to determine whether it was an appropriate time to settle the case (Purpose A). Those rights and entitlements are irrelevant to the argument that the DOH could process personal data for the purposes of seeking to determine an appropriate time to settle the case.

6.90. Against that, the DOH has provided no evidence that it considered the impact of the processing on data subject rights. Its legal advice received in 2017 made no reference to these rights or the impact of the processing. When asked if it had assessed the impact of the processing on data subjects, the DOH answered in the negative. In 54 pages of submissions on the Draft Decision, the DOH did not include any submission to demonstrate that its ongoing processing under GDPR was proportionate to the right to data protection.

6.91. The DOH also submitted that (DOH's emphasis):

> the crux of the finding on proportionality is that the information sought was disproportionate because of its scope and the duration of its retention. This is entirely at odds with the duty of

[61] DOH's Submissions of 9 March 2023, [134.b]

> a party to litigation to identify and preserve 'data which **may be of relevance** to the matter and to suspend routine/automatic data destruction processes.' Orla McNulty v The Governor and Company of the Bank of Ireland t/a Bank of Ireland Group, [2021] IECA 182. Undoubtedly the data (i.e. service updates) "may be of relevance" to the litigation – which concerns the adequacy of services – and that being so, the Department cannot be faulted for preserving the data on its litigation files.[62]

6.92. The crux of the finding on proportionality in the Draft Decision could not be characterised in that way. It considered a number of other aspects of the proportionality test in addition, including the requirements that the processing be foreseeable and expected by data subjects, the fact that it included special category data, the vulnerability of data subjects, the fact that the information was sensitive and confidential by nature and the length of time that had passed between the initiation of litigation and the collection of the information.[63] The DOH's submissions that the finding is at odds with its duty to identify and preserve data which may be of relevance to the matter and to suspend routine data destruction processes is not relevant to processing that was not carried out for those purposes. A requirement to suspend data destruction cannot be considered to permit processing for unrelated purposes, such as determining an appropriate time to settle disputes.

6.93. I note that in addition to the processing meeting the proportionality test articulated by the CJEU, processing that constitutes a re-purposing of information must be conducted in compliance with the purpose limitation principle in Article 5(1)(b) GDPR. That principle is given further effect by Article 6(4) GDPR which requires the controller to conduct an assessment of whether the new purpose is compatible with the earlier purpose, having regard to a link between the purposes for which the data have been collected and the intended further processing; the context in which the personal data have been collected, in particular regarding the relationship between the data subjects and the controller; the nature of the personal data, in particular whether special categories of personal data are process; the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.

6.94. The processing amounted to a serious interference with the rights to privacy and data protection of the affected data subjects: the plaintiffs and their family members. The processing took place based on a detailed catch-all request to the HSE asking for any information that it thought would be relevant to share. The information provided included details that went beyond the services that the DOH actually provided, and included details of the private life circumstances of the plaintiffs and their families. It was collected in a context of litigation that had been dormant for a long period of time, which means that it would not be reasonably expected by data subjects that the information would be used for those purposes. It was collected in a context where there was an expectation of confidentiality on the part of data subjects. It was also stored with other information that had been received about plaintiffs,

[62] DOH's Submissions of 9 March 2023, [134.c]
[63] Draft Decision, [10.53]-[10.57]

including educational profiles that had been shared by the DOE. This resulted in the DOH holding a detailed profile of data subjects' health and education in a context where it had initiated litigation up to twenty years previously. In many cases, the plaintiffs were children when the case was initiated and adults by the time of the information sharing. The cases were initiated on their behalf, and the idea that they had put the services at issue themselves is therefore illogical. Only certain purposes in the public interest can justify such a serious interference with the rights of data subjects. Those purposes include serious crime.[64] They do not include the state seeking to obtain a more financially beneficial outcome in public interest litigation. Therefore, I find that the processing amounted to a disproportionate interference with the rights of data subjects.

6.95. The DOH also claimed that the Draft Decision erred in law by failing to consider the Department's protections in the context of litigation. In this regard, it relied on *GC v CNIL* wherein the CJEU held that the right to privacy under Article 7 of the Charter must be balanced against other fundamental rights. In that case, the CJEU went on to say (emphasis added):

> **While the data subject's rights protected by Articles 7 and 8 of the Charter override, as a general rule, the freedom of information of internet users**, that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

6.96. The DOH also relied on Case C-336/19, *Centraal Israelitisch Consistorie van Belgie ea* EU:C:2020:1031, which stated at [56]:

> Where several fundamental rights and principles enshrined in the Treaties are at issue, such as, in the present case, the right guaranteed in Article 10 of the Charter and animal welfare enshrined in Article 13 TFEU¸ **the assessment of observance of the principle of proportionality must be carried out in accordance with the need to reconcile the requirements of the protection of those various rights and principles at issue, striking a fair balance between them** (see, to that effect, judgment of 19 December 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114 paragraph 50 and the case-law cited).

6.97. The DOH continued, "*the Draft Decision is therefore also vitiated by error of law in its failure to conduct a proper proportionality analysis by entirely overlooking the competing rights and interests at stake in this context*."

6.98. It is inaccurate to say that the Draft Decision overlooked any rights and interests. It considered the issue of necessity to legal advice or litigation at length.[65] It concluded that the interests that the DOH had identified in relation to the management of litigation were outweighed by the rights of data subjects. In any event, the DOH did not, in its submissions on this issue, include

[64] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis*, Judgment of 21 December 2016 ('Tele2 Sverige AB'), [115]

[65] See analysis of Issue 3 in the Draft Decision

any reference to rights or entitlements of litigants that relate to obtaining information to determine appropriate times to settle cases. It include detailed submissions on the rights and entitlements of litigants to obtain documents for evidential purposes or to put in place litigation holds. The DOH failed to acknowledge that it is its responsibility to conduct a proportionality analysis.

Conclusion on proportionality: On the basis of the analysis above, I consider that the DOH's processing of personal data about the private lives of plaintiffs and their families in Category A was disproportionate to the aims pursued in processing for Purpose A.

Public interest and reasons of substantial public interest under Article 23(1) GDPR

6.99. The Draft Decision engaged in a short analysis of the public interest as it applied to the DOH's processing at paragraph 10.15. However, I find that I must engage in a more detailed analysis in light of the statements about this issue in the DOH's submission on the Draft Decision that contradict its earlier submissions and call into question its assessment of the public interest.

6.100. Originally, the DOH said, "*there was no evidence*" to support the allegation on Prime Time that "*sensitive personal information was being used against families, to leverage a more beneficial outcome for the State*."[66] By contrast with the position that personal information was *not* being used by the DOH to leverage a more beneficial outcome for the state, in its 9 March 2022 submissions the DOH said that the context in which updates were sought from the HSE was "*to ensure that there was not inappropriate or premature reactivation of the case. [sic] that could lead to a negative impact on the public purse*."[67] These contradictions were put to the DOH in August 2022, to allow it an additional opportunity to reply. DOH said, "*there is no contradiction in the submissions made. The Department does not deny or shy away from the fact that there is always a need to preserve public funds and to avoid unnecessary expenditure when conducting litigation*."[68]

6.101. Article 6(1)(e) GDPR specifies that processing must be in the public interest, and Article 6(3) GDPR states that processing on the basis of 6(1)(c) or (e) must be on the basis of a public interest in Article 23(1) GDPR. It is also expressly required by section 38(1)(a) of the 2018 Act and section 40C of the Health Act 2004 that processing is for a public interest purpose. The DOH has now made an issue of public interest by claiming that the processing was to preserve public funds. The DOH's explanations of the public interest in its submissions and the documentation reviewed by the Case Officers focus solely on the financial implications of the processing for the DOH, which is one aspect of the public interest. The DOH did not include details of how it considered other relevant aspects of the public interest, including those that are derived from its overall mission and functions. The DOH's describes its own overall mission and functions as

[66] October 2021 Submissions
[67] DOH's Submissions 9 March 2022, [31]
[68] Letter of 14 October 2022, p6

providing a person-centred health service for individuals in the state.[69] Thus, it is in the public interest that individuals can seek to hold the DOH to account for the delivery of health services in the court. As noted by Murphy J extra judicially in a recent academic publication,

> The State is not an ordinary party involved in adversarial proceedings; rather the State is the ultimate guarantor of the rights of its citizens, and therefore, its role in litigation ought to be viewed through that prism.[70]

6.102. It is also in the public interest that individuals receive appropriate sums in settlement. These aspects of the public interest were not considered by the DOH. It appears to have viewed SENs litigation purely as a financial burden on the state.

6.103. In failing to consider the impact of the processing on data protection, the DOH also failed to consider another important aspect of the public interest. There is a public interest in members of the public being able to receive health and educational services on the understanding that their personal data collected in those contexts will be treated confidentially and for the purposes for which they were collected. A lack of confidence on the part of the public that state departments will respect the confidential context in which that information was collected can impact the ability of the public to avail of those services at all. Individuals may hold back information that would be relevant to share with professionals if they believe that it will subsequently be used for unrelated purposes. The public interest in the ability to receive certain services in confidence has been expressly recognised by the Supreme Court. In *National Irish Bank v RTÉ*, Lynch J stated in relation to the duty of confidence that exists in many relationships, including between bankers, doctors, lawyers and their clients:

> There is a public interest in the maintenance of such confidentiality for the benefit of society at large.[71]

Conclusion on public interest: I find that the DOH did not appropriately assess the public interest in processing, by failing to take data subject rights into consideration prior to engaging in processing for Purpose A.

iii. <u>Conclusion on processing personal data in Categories A and B(i) for Purpose A</u>

6.104. In summary of the foregoing findings, I find that it was disproportionate and excessive to process certain information in Category A for the sole purposes of seeking to determine whether it was an appropriate time to seek a settlement in litigation.

6.105. To summarise the thrust of the DOH's submissions, it interpreted its rights or obligations as a state litigant to both keep the case moving and also to avoid probing the case at the wrong time,

[69] October 2021 Submissions, 1
[70] Murphy, "The Role and Responsibility of the State in Litigation" 5. Deirdre Murphy et al.pdf (ijsj.ie)
[71] *National Irish Bank v RTÉ* [1998] 2 IR 465, 494 quoted by Kelleher D in *Privacy and Data Protection Law in Ireland*, Bloomsbury 2015, at [9.45]

which could lead to state expenditure that exceeded a settlement pay out at a time when the litigant was happy with the services that were the subject of the litigation. This is not a purpose that ties directly to preparing a defence in legal proceedings. It does not derive from any of the rights or entitlements of litigants referenced by the DOH. It is a purpose that relates to state expenditure on litigation rather than relating directly to the litigation itself. Those factors do not preclude the DOH's purposes from falling within the broadly worded provisions of the 2018 Act or the DOH's broad statutory functions, including those that permit information sharing with the HSE. From an EU law perspective, those provisions could benefit from further clarity, precision and foreseeability. While the personal data that will be relevant to any particular context for seeking legal advice or defending litigation will naturally be a function of that context, I do not consider it to be made out that those legal provisions can justify the re-purposing of information held by the state to provide services to members of the public to determine whether it is an appropriate time to settle the case. In the analysis of necessity above, I considered whether the DOH could meet the EU law threshold for necessity in the context of processing for Purpose A. As the DOH had been "letting the cases lie" for nearly a decade or more, there was no perceived urgency on its part to settle the cases in question. At most, based on the arguments made by the DOH, there was a need to dispense with the case at the most financially advantageous time for the state, by virtue of the DOH's position as a defendant in litigation and a safeguarder of public funds. I ultimately found that the DOH could not meet the test for strict necessity where there were other means of processing less intrusive to data subject rights that would also contribute effectively to its aims.

6.106. Overall, I find it disproportionate to data subjects' right to data protection to engage in scoping exercises for this narrow purpose. In coming to this conclusion, I have carefully considered the balance between data subject rights and the right of the DOH to engage in litigation and seek legal advice. This processing purpose was unconnected to the preparation of a defence, nor was it carried out so the DOH could maintain a file of information pursuant to an obligation to put in place a litigation hold. Its ability to seek advice about the legal aspects of settlements was not contingent upon its receipt of this information. Against that, the information had been collected in the course of the provision of health services to litigants. The cases had been dormant for so long that the litigants had been children when the cases were initiated in their name, and adults by the time information was collected. Most litigants also will not have the resources of the state at their disposal to find out information about plaintiffs' private lives that could be beneficial in identifying financially advantageous times to take action on a case. The litigation was taken in order to avail of services that it is within the DOH's mission to provide. In the context of this type of litigation, there are competing public interests that the DOH had to balance – its budget and the services it provides, and its accountability for providing those services. There is also a public interest in the public being able to share personal details with service providers without unexpected re-use being made of that information. Above all else, there is no evidence that the DOH ever considered the impact of its practices on data subjects. As controller, it was its responsibility to make this assessment before the processing commenced or continued under the GDPR.

6.107. I therefore find that the DOH infringed Articles 6(1), 6(4) and 9(1) GDPR in processing certain personal data for Purpose A, as outlined specifically in paragraphs 6.109 and 6.110.

6.108. I find that the DOH infringed the principle of data minimisation in Article 5(1)(c) GDPR in relation to the information received and processed in response to question 4 of its template request to the HSE, on the basis of the analysis outlined in paragraphs 6.63 to 6.76 above.

6.109. I have also considered whether this conclusion should apply to all the information in categories A and B(i), or just to the "excessive" information collected in connection with category A. I find the "excessive" information alone was disproportionate.

6.110. I find the other information in categories A and B(i) could have been collected for Purpose A, as it is reasonable for a state department subject to litigation to identify which services are still being received by a plaintiff in open litigation, in the context of determining whether to settle a case. I do not find that this processing infringed Articles 5(1)(c), 6(1)(e), 6(4) or 9(1) GDPR.

iv. <u>Conclusion on processing personal data in Categories A and B for Purpose B</u>

6.111. I make no finding of infringement with regard to retention or other processing of information in Categories A or B by the DOH for Purpose B.

6.112. In coming to this conclusion, I note the following aspects of the DOH's submissions:

> [45]… There is an ongoing need to retain information which provides a point-in-time snapshot of the key issues in the case, which may then be essential later on in the case, depending on Counsel's advice (on which latter point see the discussion under Issue 2) and on the evolution of the litigation (which cannot be predicted with precision in advance). The Department submits that it is important to be able to trace developments in a case in order to ascertain exposure to quantum and/or likelihood of a resource-related remedy being awarded (directing a certain level of care) by the Court.
>
> …
>
> [70] The Draft Decision appears to impose a requirement that the Department should assess each document containing personal data it receives, which is held on a litigation file, to determine whether it is necessary to the defence of the proceedings. However, it is a matter for Counsel to advise on proofs; including all documents which are necessary for defence of a case. Furthermore, it would impose a disproportionate burden (financial and otherwise) on

any litigant to seek advice from Counsel on an ongoing basis as regards the necessity for retention of each document it receives.

…

[102] … the destruction by a party to proceedings of relevant documents – as appears to be countenanced by the Draft Decision – may lead to adverse inferences being drawn against that party at trial. (See, for example, Infabrics Ltd v Jaytex Ltd [1985] F.S.R. 75.)

…

[103] the Court of Appeal has recently confirmed the extent of the obligation of a party to *civil proceedings* – such as the Department– to retain potentially relevant documents. *In Orla McNulty v The Governor and Company of the Bank of Ireland t/a Bank of Ireland Group*, [2021] IECA 182, the Court of Appeal (Collins J.) made the following comments (emphasis added)…

> …
>
> *In my view, litigants are obliged to take reasonable steps to preserve relevant documentation (including ESI) so as to ensure its availability on discovery and their legal advisors – whether internal or external – have a duty to advise their clients of this obligation. As advised by the Good Practice Discovery Guide, the issue of what document and information ought to be preserved may need to be reviewed in the course of litigation, as for instance where amendments to pleadings are sought to be made.* ***It is not sufficient to address issues of preservation only at the point discovery is requested or when discovery is ordered.*** *There may be – and frequently will be – a significant gap between the commencement of proceedings and the finalisation of the parameters of discovery, whether by agreement or by court order. Here, discovery was first requested more than 5 years after the commencement of the proceedings and, by the time it was agreed, almost 7 years had elapsed since commencement. That is not satisfactory on any view and, one hopes, represents the exception rather than the rule. But even where litigation is prosecuted with all due expedition by all of the parties to it, months and years may elapse before the scope of the discovery is definitively resolved.*
>
> *I emphasise that a party is required only to take reasonable steps to preserve relevant documents. What is reasonable will depend on all of the circumstances. Relevant considerations will include the nature and scope of the proceedings, the extent of the universe of potentially relevant documents and the number of potential custodians. The experience and resources of the parties, and whether they are legally represented or not, will also be relevant. Whether and to what extent these issues have been addressed in prior correspondence may also be relevant. It is open to a party or their legal advisors to write at an early stage in litigation (or even before its commencement) identifying categories of documents likely to be the subject of a discovery request in due course and expressly putting the other party on notice of the*

need to take steps to preserve such documents. That is frequently done in practice, though it does not appear to have done here.

6.113. Having considered these submissions, without prejudice to the findings relating to processing for Purpose A, I recognise that there is a variety of reasons why the DOH would need to retain information relating to litigation and for archiving purposes, regardless of whether it was otherwise lawfully collected or processed. I do not make any finding that its retention practices complied with the GDPR. However, I do not find that there is sufficient evidence to make a finding that its practices relating to the retention of personal data in Categories A or B for Purpose B infringed the GDPR.

6.114. In it submissions dated 6 June 2023, the DOH indicated that it accepted the above findings:

> The Department accepts your provisional findings of pp 6.107 -6.11 O that "DOH infringed the principle of data minimisation in Article 5(1)(c) GDPR in relation to the information received and processed in response to question 4 of its template request to the HSE." We also welcome your findings that the "excessive" information alone was disproportionate, and that "it is reasonable for a state department subject to litigation to identify which services are still being received by a plaintiff in open litigation, in the context of determining whether to settle a case."[72]

7. Issue B: Whether the DOH may legitimately rely on Article 23 GDPR and section 60(3)(a)(iv) or 162 of the 2018 Act to restrict the scope of the obligations of Article 14 GDPR to provide transparent information to data subjects in respect of SENs cases where personal information concerning data subjects is obtained from sources other than the data subjects

7.1. This issue concerns whether the DOH may legitimately rely on Article 23 GDPR and section 60(3)(a)(iv) or 162 of the 2018 Act to restrict the scope of the obligations of Article 14 GDPR to provide transparent information to data subjects in respect of SENs cases where personal information concerning data subjects is obtained from sources other than the data subjects.

7.2. This Decision focusses on the information that was contained in the DOH's privacy policy and whether that information included descriptions of the processing that was carried out by the DOH. To the extent that any processing purposes, data categories or recipients were not outlined in the privacy policy, it will be considered whether the DOH can rely on applicable exemptions in relation to these.

i. Relevant law

EU Law

7.3. Recitals 39 and 58 GDPR state:

> (39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise

[72] DOH's Submissions 6 June 2023, page 4

processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

7.4. Article 5 GDPR states, in paragraph 1 thereof:

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subjects ('lawfulness, fairness and transparency')

…

7.5. Article 12 GDPR states:

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear

and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

7.6. Article 14 GDPR states:

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

7.7. Article 23 GDPR, entitled ‘Restrictions’, provides:

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

…

(f) the protection of judicial independence and judicial proceedings;

…

(j) the enforcement of civil law claims.

…

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Relevant EU case law

7.8. In *La Quadrature du Net,* Joined Cases C-511/18, C-512/18 and C-520/18, Judgment of 6 October 2020, the CJEU held,

> [209] With regard, more specifically, to Article 23(1) of Regulation 2016/679, that provision, much like Article 15(1) of Directive 2002/58, allows Member States to restrict, for the purposes of the objectives that it provides for and by means of legislative measures, the scope of the obligations and rights that are referred to therein 'when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard' the objective pursued. Any legislative measure adopted on

that basis must, in particular, comply with the specific requirements set out in Article 23(2) of that regulation.

[210] Accordingly, Article 23(1) and (2) of Regulation 2016/679 cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein (see, by analogy, with regard to Directive 95/46, judgment of 20 May 2003, Österreichischer Rundfunk and Others, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 91). In particular, as is the case for Article 15(1) of Directive 2002/58, the power conferred on Member States by Article 23(1) of Regulation 2016/679 may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (see, by analogy, with regard to Directive 95/46, judgment of 7 November 2013, IPI, C-473/12, EU:C:2013:715, paragraph 39 and the case-law cited).

[211] It follows that the findings and assessments made in the context of the answer given to question 1 in each of Cases C-511/18 and C-512/18 and to questions 1 and 2 in Case C-520/18 apply, mutatis mutandis, to Article 23 of Regulation 2016/679.

7.9. In *Smaranda Bara,* Case C-201/14, Judgment of 1 October 2015, it was held:

> [47] Articles 10, 11 and 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body of a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects having been informed of that transfer or processing.

7.10. Article 10, 11 and 13 of Directive 95/46/EC are the equivalent of Articles 13, 14 and 23 GDPR.

Irish Law

Data Protection Act 2018

7.11. Section 60 of the 2018 Act, entitled 'Restrictions on obligations of controllers and rights of data subjects for important objectives of general public interest' in subparagraph 3 states,

> Subject to subsection (4), the rights and obligations referred to in subsection (1) are restricted to the extent that—
>
> (a) the restrictions are necessary and proportionate—
>
> …
>
> (iv) in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure,

…

7.12. Section 162 of the 2018 Act, entitled 'Legal privilege' states,

> The rights and obligations provided for in-
>
> (a) Articles 12 to 22 and 34 of the Data Protection Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22),
>
> …
>
> do not apply—
>
> (i) to personal data processed for the purpose of seeking, receiving or giving legal advice,
>
> (ii) to personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings, including personal data consisting of communications between a client and his or her legal advisers or between those advisers, or
>
> (iii) where the exercise of such rights or performance of such obligations would constitute a contempt of court.

Legal professional privilege ('**LPP**')

7.13. LPP can be separated into two categories: legal advice privilege and litigation privilege. The purpose of legal advice privilege is to protect confidential communications between a solicitor and their client at any time. Litigation privilege protects advice and other documents connected to confidential preparations for litigation.

7.14. The test for litigation privilege has recently been restated by the Irish courts in the case of *Lehane v Yesreb Holding and Celtic Trustees Limited*.

> The client must establish that what is sought to be protected is a communication, whether written or oral, that is made:
>
> - between either (i) himself or (ii) his lawyer (who is acting for him in a professional capacity) and a third party;
> - in either case under conditions of confidentiality;
> - for the dominant purpose of use in litigation, thus, that at the time the communication is made (i) is either preceding or pending, or reasonably anticipated or in contemplation, and (ii) is litigation in which the client is, or reasonably anticipates, becoming a party; and
> - for the purpose of either (i) enabling legal advice to be either sought or given and for/or (ii) seeking or obtaining information to be used in or in connection with the litigation concerned.[73]

7.15. In relation to the dominant purpose test, the *Lehane* judgment goes on to describe further elements.[74] First, the document must have been created when litigation is apprehended or threatened. Secondly, the document must have been created for the dominant purpose of the apprehended or threatened litigation; it is not sufficient that the document has two equal purposes, one of which is apprehended or threatened litigation. Thirdly, the dominant purpose of the document is a matter for objective determination by the Court in all the circumstances and does not only depend upon the motivation of the person who caused the document to be created.[75] The onus is on the party asserting privilege to prove, on the balance of probabilities, that the dominant purpose for which the document was brought into existence was to obtain legal advice or enable his solicitor to prosecute or defend an action.[76]

7.16. The test for legal advice privilege has been summarised by Abrahamson, Dwyer and Fitzpatrick as follows:

> The authorities reveal that, in order to attract legal advice privilege, the material in question must satisfy a number of criteria.
> (a) First, the material must constitute or refer to a communication between lawyer and client.
>
> (b) Secondly, that communication must arise in the course of the professional lawyer–client relationship.
>
> (c) Thirdly, the communication must be confidential in nature.
>
> (d) Fourthly, it must be for the purpose of giving or receiving legal advice.[77]

[73] [2018] IEHC 745, [34] quoting Passmore on Privilege (2013) at p213
[74] Ibid at [35] citing *University College Cork v Electricity Supply Board* [2014] 2 IR 255 at 529
[75] Ibid, citing *Gallagher v Stanley* [1998] 2 IR 267 at p.274
[76] Ibid, citing *Woori Bank and Downey v Murray* [1988] NI 600
[77] Discovery and Disclosure, Round Hall, 3rd Edn, 2019, [40.16]

ii. Relevant Facts

7.17. On 14 October 2022, the DOH stated that its (undated) privacy policy contained the following statements:

> Under "Purpose and Legal Basis for Processing", it provides:
>
> "*The department needs to process certain personal data to carry out the tasks required for the performance of its functions and to comply with certain legal obligations. We also process personal data received from members of the public who contact us so that we can provide them with the services they require.*
>
> *Processing of Information takes place for the following purposes:*
> - *processing necessary to meet obligations provided for in legislation …*
> - *processing relating to discovery of records, access to the institutional and related records (AIRR), statutory committees of investigation and litigation…*
> - *processing necessary to respond to queries and requests for information from patients/family members, members of the public, third parties such as solicitors, elected representatives, interest groups and other stakeholders…*
>
> *Most of the personal data processing by this department is carried out for the performance of the Minister's functions or in the public interest*."
>
> Under "Types of personal data collected by the Department" it provides:
>
> *"Reason… Litigation/Statutory Committees of Investigation…*
>
> *Categories of Personal Data Collected: Personal data, including contact details and medical and family history, contained in records relating to litigation/statutory committees of investigation, in which department is involved. In some instances, financial details necessary to facilitate payments."*
>
> Under "How the Department collected Personal Data", it provides:
>
> *"Directly from individuals*
>
> *The department collects personal data directly from members of the public, patients and their family members and third-party representatives such as Solicitors, and lobby/interest groups. This data may be received by phone, email or written correspondence. It may also be obtained through public consultations….*
>
> *State Agencies*
> *The Health Service Executive and other State Agencies under the aegis of the department disclose data to the department in the performance of their functions. Information includes data required to support the management of the service in question, governance activities, appointments to Committees/Boards, information relating to human resources policies and procedures, information relating to legal cases against the State and contact details for mailing lists and so on….*

Other Public Bodies
The department liaises with a wide range of government departments and agencies in order to perform its functions, for example:

- *information regarding legal cases is received from the Chief State's Solicitors Office, the State Claims Agency, Tribunals of Inquiry…"*

Under "Who the Department shares personal data with" it provides:

"In some instances, personal information held by the department is shared with other government departments/Agencies to enable the department to perform its functions. In such cases the disclosure is made in a manner consistent with the original purpose for which the information was provided."

7.18. The DOH said, "the Department provided information publicly about its processing of personal data which is consistent with the practices involved in SEN litigation."[78]

iii. Analysis of Issue B

7.19. The full text of Article 14 is outlined above, and it creates an obligation to provide various pieces of information where personal data are not obtained from the data subject. Those include in subparagraph 1:

> …
>
> (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
>
> (d) the categories of personal data concerned;
>
> (e) the recipients or categories of recipients of the personal data, if any;
>
> …

7.20. Under Article 14(2), the controller must also provide details of:

> (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

7.21. Looking at the requirement to provide information about the purposes of processing under Article 14(1)(c) first, in relation to SENs litigation, the DOH's policy makes some broad references to litigation and the performance of its functions. In relation to the categories of information required by Article 14(1)(d), the DOH say that the categories of personal data it may use for litigation include: "*Personal data, including contact details and medical and family history, contained in records relating to litigation/statutory committees of investigation, in which department is involved. In some instances, financial details necessary to facilitate*

[78] Letter of 14 October 2022, p10

payments." This explains that personal data including medical and family history contained in litigation records will be processed. It does not state that medical and family history originally contained in other records will be repurposed and processed for litigation purposes.

7.22. In relation to recipients and sources of personal data, details of which are required to be provided under Articles 14(1)(e) and 14(2)(f) GDPR, the privacy policy states that information relating to legal cases will be obtained from "*the Chief State's Solicitors Office, the State Claims Agency, Tribunals of Inquiry*." It states that the DOH may share information it holds with other government agencies and departments.

7.23. Article 12(1) requires information provided under Article 14 to be provided in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*." Interpreting these requirements, the Article 29 Working Party Guidelines on Transparency state:

> The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations.

The information provided under Article 14(1)(c) should be provided in such a way that there is a clear link from:

> a. a specified category/specified categories of personal data, to
> b. the purpose(s) of the specified processing operation/set of operations, and to
> c. the legal basis being relied upon to support that processing operation/set of operations.[79]

7.24. The following details about the DOH's practices are not evident from the information outlined above. These practices are described in the DOH's own words, and were notably included in a report that was made public following the Whistleblower's allegations:

- In addition, in the course of its defence of the litigation the Department of Health sought service updates from the HSE (co-defendant) from time to time… Service updates are retained on the litigation files. The Department had been advised that in the absence of service updates, it would be difficult to advise on the settlement of cases.

- It is in the public interest that State parties to litigation manage those proceedings as efficiently as possible. In pursuing a well-managed approach to litigation in the public interest, Government Departments regularly adopt a joint strategy in defending litigation. Indeed, it is normal practice for defendants to litigation to co-operate and share appropriate information with each other required for obtaining legal advice and/or defending the proceedings, where they have a common interest in the issues and outcome of the proceedings. Such an approach is necessary to protect the State's legal rights, facilitates effective engagement between all parties to the litigation, including the plaintiff, and ultimately serves the public interest.

7.25. It is inaccurate for the DOH to say that the information that it provided in its public privacy notice was consistent with the practices involved in SEN litigation. The reference to sharing

[79] WhatsApp Decision, [302]

between government departments in the DOH's privacy policy says the "*the disclosure is made in a manner consistent with the original purpose for which the information was provided*." That sentence plainly indicates that personal data collected by one government agency will be shared for the same or consistent purposes. It does not convey that information would be shared for litigation purposes. Government departments were not included in the list of entities from which the DOH may receive information relating to legal cases. The fact that the DOH would receive educational reports from the DOE or seek service updates from the HSE was not evident from the DOH's privacy notice. The closest it got was to say that the HSE would disclose information "*relating to legal cases*." It did not say that the HSE would disclose private or family information collected in the course of providing health services for the purposes of legal cases.

7.26. Therefore, the DOH did not provide all of the information required to be provided to data subjects under Articles 14(1)(c)-(e) and 14(2)(f) GDPR.

7.27. The DOH has consistently maintained that it could rely on section 60(3)(a)(iv) of the 2018 Act to not provide further information to data subjects, stating,

> It could never be routing [sic] practice for defendants and co-defendants to inform a plaintiff of legal defence and settlement processes and considerations and disclosure of such information would undermine a party's ability to defend itself…
>
> The processing of personal data in the context of these cases relate to the defence of legal claims and/or legal proceedings before the courts. The creation of files and records in SEN cases exclusively and directly flows from the initiation of such legal claims and/or proceedings (i.e. the nature of the processing of personal data in the context of these files would not exist but for creation of the legal claims and/or proceedings). As such, the Department's clear position is that it may legitimately and lawfully rely on Article 23 GDPR and Section 60(3)(a)(iv) of the Data Protection Act 2018 in this context.[80]

7.28. As noted at paragraph 14.20 of the Draft Decision, Article 14 GDPR requires controllers to provide general information to data subjects about data processing, and does not require the full content of the personal data processed to be disclosed to the data subject. The general information that was provided by the DOH in its privacy policy did not include details of its processing practices that would allow members of the public to understand the practices that were taking place.

7.29. I consider that the DOH could not rely on any exemptions to avoid providing this generalised information about its practices.

7.30. Data subject rights restrictions set out in the 2018 Act must be necessary and proportionate for the objective pursued, in line with both Article 23(1) and the principles of EU law more generally. Looking first at LPP, while the words "*necessary and proportionate*" are not included in section 162 of the 2018 Act, that section is an implementation of Article 23 GDPR, which

[80] DOH's Submission on Inquiry Issues Paper, 4 October 2021, p20

requires all restrictions on data subject rights to be necessary and proportionate. More generally, any derogations from rights protected by the CFR must be necessary and proportionate to the aim pursued.[81] The principles of necessity and proportionality remain to be considered by the Irish courts in the context of LPP. However, the meaning of those terms in the context of CJEU case law summarised in the issue dealing with lawful basis apply in this context. Necessity is an assessment of the aim pursued, and proportionality is an effort to seek to balance the legitimacy of that aim against the rights of data subjects. LPP has, in itself, been considered to be interlinked with the fundamental right to privacy.[82] In that regard, the CJEU case law relating to the balance of another freedom against the fundamental right to data protection is instructive. In *Satamedia*, it was held that,

> In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly. Secondly, and in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary.[83]

7.31. The broader objective of LPP is "*the public interest in proper conduct of the administration of justice*."[84] Litigation privilege allows a party to litigation to prepare its case in confidence, and prevents the disclosure of documents that relate to the preparation of that case. In order for it to be necessary and proportionate to restrict data subject rights for the purposes of LPP, there should therefore be a connection to those broader aims of LPP. Legal advice privilege seeks to ensure that communications between a lawyer and client remain confidential.

7.32. Section 60(3)(a)(iv) restricts data subject rights

> to the extent that
>
> > the restrictions are necessary and proportionate -
> >
> > > in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure.

7.33. Based on these exemptions, defendants in litigation would not generally be expected to contact plaintiffs to tell them what documents they hold about them that relate to the action. However, I consider that it would have been proportionate for the DOH to have, at the least, included

[81] Article 52(1), CFR
[82] *Holyoake v Candy* [2017] EWHC 52 (QB) [92]
[83] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy*, Judgment of 16 December 2008, [56] Note that data protection rights were defined in terms of 'privacy' in the Data Protection Directive 95/46 –this is not the case in the GDPR.
[84] *Smurfit Paribas Bank v AAB Export Finance Ltd* [1990] 1 IR 469, [26]

summary information on its website about its practices in relation to litigation that were outlined at paragraph 7.24. There is no reason why this would prejudice the outcome of any specific case, or cause damage to any other rights or entitlements of litigants considered above in the section relating to lawful basis. Providing summary information would not require the DOH to disclose the contents of any specific privileged communication.

7.34. In reality, in relation to Purpose A, the DOH sought to restrict the right to transparency for a specific reason. This reason was avoiding the reactivation of litigation. The DOH specifically asked that data subjects were not informed by the HSE that their personal data would be collected because that could risk reactivating the litigation that they had taken against the state, which would have defeated the overall purpose for collection. DOH has not demonstrated that it was necessary or proportionate to restrict the right to information for Purpose A.

iv. Conclusion on Issue B

For the reasons outlined above, I find that the DOH did not provide data subjects with the information required under Article 14(1)(c)-(e) GDPR. I find that the DOH could not rely on section 60(3)(a)(iv) or 162 of the 2018 Act to avoid providing summary information about its practices in its privacy policy. I also find that it was not necessary or proportionate to restrict the right to information for the reasons why the DOH actually sought to restrict this right. On this basis, I find that the DOH has infringed Article 14 GDPR by failing to provide summary information to data subjects about its practices. I find that its non-transparent re-purposing of information collected by the HSE and DOE was an infringement of Article 14.

7.35. In it submissions dated 6 June 2023, the DOH indicated that it accepted the above findings:

> In relation to Issue 8, the Department, in light of the above also accepts under the principle of transparency, that it did not "provide all of the information required to be provided to data subjects under Articles 14(1)(c)-(e) and 14(2)(f) GDPR", as outlined in pp 7.26, to provide transparent information to the data subjects in respect of SENs cases where personal information was obtained from sources other than the data subjects themselves. We note from pp 9. 14 that our reliance upon section 38(1) of the 2018 Act to collect information from other public bodies, can no longer form a basis for processing because it has disapplied following commencement of section 6(2) of the 2019 Data Sharing and Governance Act.
>
> We also accept your provisional finding that "DOH could not rely on any exemptions to avoid providing this generalised information about its practice" and accept that it would have been proportionate for the Department to have outlined in the summary information on our website about our practices in relation to further data processing for the purposes of litigation.[85]

8. Issue C: Whether the DOH complied with its obligations under Articles 5(1)(f) and 32(1) GDPR

[85] DOH's Submissions 6 June 2023, pages 4-5

in relation to the internal access to its litigation files

i. Principle of integrity and confidentiality

8.1. Article 5(1)(f) GDPR provides for the principle of integrity and confidentiality. It requires that personal data shall be:

> processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8.2. Article 32(1) GDPR elaborates on the principle of integrity and confidentiality in Article 5(1)(f) by setting out criteria for assessing what constitutes '*appropriate security*' and '*appropriate technical or organisational measures*':

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> a) the pseudonymisation and encryption of personal data;
>
> b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.3. Articles 5(1)(f) and 32(1) GDPR oblige controllers and processors to implement a level of security appropriate to the risks presented by its processing of personal data. There is an obligation to consider the "*state of the art*" with regard to measures available. The term "*state of the art*" is not defined in the GDPR. By dictionary, it is defined as "*using the latest techniques or equipment*."[86]

8.4. The term "*state of the art*" has been considered by the EDPB in its Guidelines on Article 25 GDPR. These Guidelines state that it imposes an obligation on controllers "to take account of

[86] Concise Oxford Dictionary, (8th ed., BCA & Oxford University Press, 1991)

the current progress in technology that is available in the market" and "how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape."[87]

ii. Assessing Risk

8.5. Articles 5(1)(f) and 32(1) GDPR oblige controllers and processors to implement an appropriate level of security. The level of security must be appropriate to the risk presented to the rights and freedoms of natural persons, and must have regard to the state of the art, the costs of implementation and the nature scope, context and purposes of processing. Therefore, the first step is to assess the risk presented to the rights and freedoms of data subjects by the processing of personal data, and then to assess the appropriate security measures implemented (as detailed in the following sections (b) and (c)).

8.6. Recital 76 GDPR provides guidance as to how risk should be evaluated:

> The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

8.7. The CJEU judgment in *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and others*[88] provides further guidance on the risk assessment. In this case, the CJEU declared the Data Retention Directive[89] invalid. The Directive required electronic communication service providers to retain certain data for a period of time. The CJEU held that the Directive did not ensure effective protection of the data retained against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to:

> (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.[90]

8.8. Considering the CJEU approach, it appears that risk of processing personal data by the DOH in SENs litigation files is assessed objectively by reference to (i) the likelihood of the risk to the

[87] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (op. cit.), [19]
[88] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, Judgment of 8 April 2014 ('Digital Rights Ireland Ltd')
[89] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
[90] Digital Rights Ireland Ltd, (op. cit.), [66]

rights and freedoms of plaintiffs and their family members whose personal data are stored in SENs litigation files, and (ii) the severity of that risk. The objective assessments must be made by reference to the nature, scope, context and purposes of the processing. In considering these factors, regard must also be had to the quantity of personal data processed and the sensitivity of that data. Only in light of the risk assessment is it possible to analyse the appropriateness of the security measures implemented (as detailed in the following parts (iii) and (iv)).

8.9. The nature of personal data is at the higher end of the scale of sensitivity. It includes medical reports and other information obtained indirectly from clinicians and in one case information received from a clinician directly. Therefore, the personal data processed includes personal data concerning health, a special category of personal data under Article 9(1) GDPR. This is the case for all personal data of a medical and/or clinical nature contained in both the paper and electronic files, regardless of its source, as it is "data concerning health" as defined by Article 4(15) GDPR, and designated as a special category of personal data under Article 9(1) GDPR and section 2(1) of the 2018 Act. As the DOH has itself admitted, "[a]lmost every file contains clinical reports"[91]. The files also contain other sensitive information, such as private details about educational and healthcare services provided to plaintiffs, and in some cases, details of their private family circumstances. Moreover, it involves the processing of personal data of vulnerable data subjects in a way that data subjects would not expect their data to be processed. These personal data, by their very nature, are particularly sensitive with regard to the fundamental rights and freedoms of data subjects. Thus, the sensitive nature of personal data processed by the DOH increases the severity of the risks, as illustrated in Recital 76 GDPR.

8.10. In relation to the scope and context of the processing, the personal data in SENs litigation files relate to long-dormant litigation taken by plaintiffs by their families. The quantity of personal data processed by the DOH in its SENs litigation files is significant, as those 29 files contain documentation provided by co-defendants and the HSE and other parties to litigation over the course of more than 20 years in some cases. The personal data have been received from the plaintiffs themselves in some cases, and also from the HSE, and other government departments that are co-defendants in the proceedings.

8.11. The purposes of the DOH's processing are ostensibly for the management and defence of litigation. In relation to those purposes, it was only necessary for a limited number of staff members at the DOH to have access to the relevant files. Moreover, the purpose for which certain personal data were collected and stored were to identify whether it would be a good time to approach the plaintiffs with regard to settlement, a purpose which, as noted above, was not strictly necessary for the purposes of defending litigation.

8.12. I find that there was a high risk in severity to the rights and freedoms of natural personal arising from the processing of personal data on SENs litigation files. This high severity arose due to the

[91] DOH's Submissions on the Draft Decision, dated March 2022, at paragraph 174.

sensitive nature of personal data in question, the quantity of personal data collected and processed and the scope of that processing. I find the likelihood of the risks actually arising to the rights and freedoms of data subjects due to access to that personal data by staff members who did not have any business need accessing those documents to be moderate. While increased access to personal data increases the risk of unauthorised loss or disclosure of that personal data, those staff members were bound by obligations of confidentiality, which reduces the risk arising from their access to that personal data.

iii. Security measures implemented by the DOH: permitting access to the SENs litigation files by staff members with no business need to access those files

I. Electronic files saved on the O-Drive

8.13. The Inquiry Issues Paper states that the Case Officers were satisfied that staff who had no business need to access the SENs litigation files did have access to those files until June or July 2020, at which time access was restricted to 25 staff serving in the Services for Older People Unit. Access was further restricted in March 2021 at which time it was restricted to five staff who required access for the performance of their official duties. It says,

> At the first inspection in the Department of Health the Departmental officials confirmed that a maximum of five staff at any one time had a work role in relation to these files and these staff were in the following grades: Principal Officer (1); Assistant Principal (1); Higher Executive Officer/Administrative Officer (2); and Clerical Officer (1). The Case Officers are satisfied that these five staff had valid access to the files in both electronic and manual (paper) form on a 'need to know' basis for the performance of their official duties.

8.14. The Inquiry Issues Paper confirms that the Whistleblower was not among the five staff members who had a need to access the SENs litigation files for the performance of their duties. Despite this, it states,

> the whistleblower continued to have access to the electronic version of the SENs litigation files until June/July 2020 even though he had transferred to work in the Finance Unit of the Department of Health in December 2019.

8.15. The Inquiry Issues Paper further highlights,

> It was confirmed to the Case Officers that when the whistleblower worked in the Older Persons Projects Unit which was part of the Services for Older People Unit, in excess of twenty five staff, including the five staff aforementioned and some staff who had left the Unit, had access to the SENs electronic files on the 'O-Drive' on the computer system.

8.16. The Whistleblower told the Case Officers during an interview with him on 5 May 2021 that he was able to access the files in March/April 2020 and that he first noticed that his access to the

files was removed in July 2020 when he met with a senior counsel appointed by the DOH to review allegations made by him in a disclosure under the Protected Disclosures Act, 2014.

8.17. In its submissions, the DOH acknowledged that the continued access by anyone to their former unit's folders after moving to another unit is not in accordance with its policies and procedures. It stated that it was important to note that the Department's policies, procedures and expectations are that its staff will act with appropriate discretion even under these circumstances. It further said that as soon as it was brought to the attention of management that there might be an individual or individuals who no longer required access to the folders in questions, the matter was addressed and access to all Social Care folders was reviewed and any access that was no longer required was removed.

8.18. The DOH provided details of its practices and procedures in relation to internal access to SENs litigation files. It explained that normal practice within the DOH is that each Unit has its own folder on the DOH's shared drive. Its submissions say,

> Access to that folder must be authorised at Principal Officer level or above when an individual joins the Department. Members of a Unit must be able to share access to an area as they will be required to collaborate on work with others in their own, immediate area of work and with other Unit members across related work areas.
>
> In this case, at that time in question, two Units within the Social Care Division had access to the relevant folder and all of its subfolders. These two Units had been a single Unit previously and may of the documents retained in that folder were relevant across both Units.
>
> A fundamental aspect of the work of the Department is to service the parliamentary system and the public. The Department receives representations from TDs on behalf of individuals, receives Parliamentary Questions about individual matters and receives representations from individuals about themselves. These inevitably contain personal information which can, depending on the case, be sensitive and is almost inevitably related to health service provision. In this context, the Department takes its responsibilities towards the processing of personal data very seriously but it is also important to note that this is an everyday part of the work of the Department. Staff who join the Department are expected to treat personal data confidentially and with appropriate discretion.
>
> The Department operates strict data protection policies that are regularly reviewed by its Data Protection Officer. All Civil Servants employed by the DOH are expected to meet the highest standards with regard to conduct and behaviour and they must certify in writing that they have received and read all relevant policies.

8.19. I note the DOH's submissions on the obligation of confidentiality on staff working within that division until access was reduced to five staff members in March 2021. While the presence of a duty of confidentiality is welcomed, it should form part of overall security and integrity policies and procedures. Considering the totality of the DOH's security measures, and the weaknesses

that the DOH acknowledged[92], a duty of confidentiality in that context does not alone provide sufficient bulwark against unauthorised internal processing. It alone is not sufficient and cannot make up for the lack of specific security measures in the context of all staff (including those with no business need) having access to highly sensitive personal data.

8.20. The DOH also provided information about the fact that it has a Data Protection Officer and dedicated Data Protection Unit. It highlighted that all staff are required to complete data protection awareness training. It further submitted that the *Civil Service Code of Standards and Behaviours* sets out a framework within which civil servants must work, including their obligations under the Official Secrets Act 1963, which prohibits civil servants from communicating official information.

II. <u>Paper files</u>

8.21. In relation to the paper litigation files for the 29 SENs litigation cases, the DOH said that those files had been stored in off-site storage unless they were being actively worked with. The DOH further explained,

> Only individuals with the relevant permissions could recall those files from storage. These permissions were restricted to those working directly with the files. Although some paper files were on site at the time the discloser was working in the Unit, these had been recalled in the month or two before the discloser joined the Unit in order to conduct the 2019 service update exercise. Only paper files relevant to this exercise were recalled from storage, i.e. only paper files that related to a sub-set of the 29 cases, many of which had additional paper files that remained in storage. There was a key for the cabinet in which these folders were held. However, due to staff departures, it has proven difficult to validate exactly what the arrangements were in place in relation to the cabinet and the key during a typical working day.
>
> It may also be noted that normal working practice within the Department is that individuals are not expected to access the cabinets that belong to other Units. In this case, the open plan nature of the area where the cabinets are located acts as a natural deterrent to inappropriate access of files.

8.22. Thus, the situation was summarised as follows in the Inquiry Issues Paper:

> Paper files relating to these cases are generally stored offsite. However, when being actively worked on, the relevant files are recalled from storage by individuals with day-to-day responsibility for working with these files, who have appropriate, restricted permissions to recall these files from storage. Once onsite, these files are stored within a cabinet in the open plan area used by the Older Persons Units within Social Care. It has not been possible to verify that this cabinet was always locked except as needed to access the files. It is therefore possible that members of the Older Persons Units without direct responsibility for SEN litigation could have accessed these files if they were aware of their existence.

[92] DOH's Submissions on the Draft Decision, dated March 2022, at paragraph 187

8.23. The Inquiry Issues Paper concluded:

> The Case Officers are satisfied, therefore, that over twenty staff who had no business reason to access the SENs litigation files had access, nonetheless, to those files in electronic and manual (paper) form. This unrestricted access remained in place until June/July 2020 at which time access was restricted to twenty-five staff serving in the Services for Older People Unit. Access was further restricted in March 2021 at which time it was restricted to five staff who require access for the performance of their official duties. [On the occasion of the second inspection, the Case Officers viewed the locked storage unit in which the manual (paper) files are kept and they were satisfied on that occasion that appropriate organisational and security measures were then in place in respect of the safe custody of those files.][93]

III. Steps taken since the *Prime Time* broadcast

8.24. In relation to the steps taken since the *Prime Time* broadcast, the DOH said that,

> the electronic files have been moved to a different location with access only permitted for those who have a direct role in the day-to-day management of those files.

8.25. It said that the paper files on-site have been secured in the manner described in the italicised text at paragraph II, and also stated,

> At a Departmental level, since the Prime Time programme aired the Department has reviewed access to all folders to ensure that access is appropriate. The Department has also put in place an online system for the approval of access to folders and is rolling out the "eDocs" file management system across the Department, which allows enhanced access control for folders and documents. In addition, file auditing software was enable for the folders that contain personal information relating to these legal cases. File access is no being periodically reviewed as team members join or leave the relevant Unit.

8.26. I acknowledge and welcome improvements to the DOH's procedures in respect of restricting access to the files to only those staff with a business need to deal with the files. I note that from March 2021, only the 5 staff member who require access for the performance of their duties actually have access. While I welcome these improvements to the DOH's integrity and confidentiality processes and procedures, the fact remains that within the temporal scope of Issue C (i.e. from 25 May 2018 to March 2021), any member of staff working in the DOH's division dealing with the likes of older people, social care and disability, had access to the files. The vast majority of those with access during that period had no business need for access. Only from March 2021 did the five staff whose work directly concerned the files had access have sole access to the files, following a period from May 2018 to June/July 2020 when 25 staff members had access. Indeed, in its submissions, the DOH does not dispute that "there was room for improvement in the implementation of appropriate technical and organisational measures to

[93] At p18, square brackets in original

limit the number of staff with access to its paper and electronic litigation files and does not contest this provisional finding"[94].

8.27. Indeed, in the context of staff members without a business need having access to the personal data, such a duty of confidentiality could be seen as an act of mitigation (as well as a security measure in the context of staff who **had** a business need for access), in that staff without a business need to access data already had access to documents to which they should not have had access. The nature of confidentiality is an obligation on staff to keep personal data confidential **after having accessed it**, whether or not they ought to have had access to the personal data. In this regard, there is a nuance between an obligation of confidentiality where staff **should have access** as part of their work, and, where they **should not have access**. While it is a security measure, a confidentiality obligation cannot cure the fact that staff had already improperly accessed certain data, and therefore is of less value as a security measure than restricting access in the first place.

8.28. In its submissions, the DOH states that the DPC failed to acknowledge, "*the majority of the information was held off-site, with on-site recall limited to a very small sub-set of directly-involved officials, for business needs*"[95]. This is acknowledged, but the fact remains that unauthorised staff members had access to both sets of files during the Temporal Scope. Therefore, this submission has not convinced me to change the finding of infringement in respect of these files.

iv. <u>The appropriate level of security</u>

8.29. Article 32(1)(d) GDPR specifies that appropriate technical and organisational measures may include regular processes for testing, assessing and evaluating. Technical measures must have, *inter alia*, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Organisational measures should enable the DOH to test, assess and evaluate the effectiveness of those measures.

8.30. Having regard to the high risk to the rights and freedoms of data subjects in terms of the severity, and the moderate risk posed by inappropriate internal access in terms of the likelihood, an appropriate level of security must include internal access restrictions that limit access to SENs litigation files to those staff members who have a business need to access the files at any given time.

8.31. In relation to electronic files, access should have been restricted to staff members who have a business need to access those files. The DOH should have had oversight of the ongoing implementation of its policies and procedures. Where staff members move to a different unit, it is not sufficient that policies state that staff should not have access to their former unit's

[94] DOH's Submissions on the Draft Decision, 9 March 2022, [178].
[95] Ibid, at [175].

folders. Those policies must be backed up by robust procedures that ensure that staff have access by business need, and that access should not follow them when they move to a different unit. This includes the implementation by the DOH of technical measures that allows it to restrict access in that way.

8.32. Thus, I consider the following to be an appropriate technical and organisational security measure:

- In addition to having organisational policies relating to security, the DOH should ensure that there are procedures in place to ensure that access is removed when staff are transferred to a different Unit, or when they no longer have any business need to access those files.

8.33. In respect of paper files, the following organisational measures are appropriate:

- The DOH should have procedures in place to ensure that files are stored offsite unless requested by a staff member who has a business need to access that file, and

- When those files are onsite at the DOH, access to the files should be restricted by locking the files in a cabinet to which only specific staff members have the access key.

8.34. These findings about appropriate security measures are without prejudice to any other conclusions in this Decision, including the conclusions about the lawfulness of processing.

8.35. The Case Officers determined that a maximum of five staff at any one time had a work role in relation to the SENs litigation files. However, until March 2021, at least 20 additional staff working in the Services for Older People Unit had access to those files. Prior to June or July 2020, staff outside of the Services for Older People Unit had access to those files also. Accordingly, I find there were inadequate technical and organisational measures in place in relation to the SENs litigation paper and electronic files on the basis of the facts outlined in relation to Issue C. I also note that the DOH did not contest this provisional finding in its submissions on the Draft Decision saying, "*there was room for improvement in the implementation of appropriate technical and organisational measures to limit the number of staff with access to its paper and electronic litigation files and does not contest this provisional finding*".[96]

8.36. I acknowledge and welcome improvements made to technical and organisational for security made since the end of the Temporal Scope of Issue C. It is acknowledged that the DOH has put in place the security measures outlined above in respect of the SENs litigation files. For the sake of clarity, it should be noted that the Temporal Scope of the matters arising in Issue C pre-dates the improvements to security put in place by the DOH.

[96] DOH's Submissions on the Draft Decision, dated March 2022, at paragraph 187

Conclusion on Issue C: I find that the DOH infringed Articles 5(1)(f) and 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its internal processing of personal data in SENs litigation files.

8.37. In it submissions dated 6 June 2023, the DOH indicated that it accepted the above findings:

> As you have noted in pp 8.11, "The purposes of the DOH's processing are ostensibly for the management and defence of litigation. In relation to those purposes, it was only necessary for a limited number of staff members at the DOH to have access to the relevant files". The Department acknowledges that there is a high risk in severity to the rights and freedoms of natural data subjects from the Department's processing of personal data on SEN litigation files. As such, the Department recognises its responsibility to protect this personal data and restrict access to it, to a specified and select number of Departmental staff with explicit business needs for accessing this data.
>
> The Department acknowledges that staff members within Services for Older Persons Unit with no business need, had access to these SEN litigation files until March 2021 when access was restricted to just 5 staff requiring it for performance of official duties.
>
> The Department has acknowledged that the whistleblower, who was positioned in the Older Persons Unit at the time was able to access data for which they had no explicit business need to access.[97]

9. Decision on corrective powers

9.1. I have set out above, pursuant to section 111(1)(a) of the 2018 Act, my decision to the effect that the DOH has infringed Articles 5(1)(c), 5(1)(f), 6(1)(e), 6(4), 9(1), 14 and 32(1) GDPR. Under section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not those findings merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

9.2. Recital 129, which acts as an aid to the interpretation of Article 58, provides that "*… each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…*" In the circumstances of the within Inquiry, and with particular reference to the findings arising therefrom, I am of the view that the exercise of corrective powers is appropriate, necessary and proportionate for the purpose of ensuring compliance with the GDPR. Having carefully considered the infringements identified in this Decision, I have decided to exercise corrective powers in accordance with section 115 of the 2018 Act and Article 58(2) GDPR. I set out below the corrective powers that I consider are appropriate to address the infringements in the

[97] DOH's Submissions 6 June 2023, page 5

particular circumstances, and the reasons for that decision, having considered all of the corrective powers set out in Article 58(2). In summary, the corrective powers that I have decided to exercise are:

a) Article 58(2)(b) – I have decided to issue a reprimand to the DOH in respect of its infringements of Articles 5(1)(c), 5(1)(f), 6(1), 6(4), 9(1), 14 and 32(1) GDPR;

b) Article 58(2)(f) – I have decided to issue a ban on processing in respect of the DOH's infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1); and

c) Article 58(2)(i) – I have decided to impose an administrative fine, pursuant to Article 83, in respect of the DOH's infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR.

A. Reprimand

9.3. I issue the DOH with a reprimand in respect of its infringements of Articles 5(1)(c), 5(1)(f), 6(1), 6(4), 9(1), 14 and 32(1) GDPR. Article 58(2)(b) provides that a supervisory authority shall have the power to "issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation." I consider that a reprimand is necessary and proportionate in view of ensuring compliance with the infringed Articles as it will act to recognise formally the serious nature of the infringements. Further, the reprimand emphasises the requirement for the DOH to take all relevant steps to ensure future compliance with the aforementioned provisions GDPR.

9.4. Recital 148 GDPR provides:

> *"In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine."*

9.5. Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. In this respect, I consider it necessary and proportionate to impose a reprimand in addition to the ban on processing and administrative fine detailed below. I have made this decision having particular regard to the nature of the infringements of Articles 5(1)(c), 5(1)(f), 6(1), 6(4), 9(1), 14 and 32(1) GDPR.

9.6. Article 5(1)(c) provides that personal data processed must be the minimum necessary for the relevant purposes, and that personal data should not be stored in a form from which data subjects can be identified for longer than necessary for the purposes for which they were

obtained. The objective of Article 6 GDPR is to ensure that personal data is lawfully processed. Article 9(2) is a derogation from the specific prohibition on processing certain special categories of personal data set out in Article 9(1). Thus, compliance with Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR are fundamental provisions that relate to whether it is lawful for a controller to hold and process personal data at all. These requirements derive from the fundamental right to data protection set out in Article 8 of the CFR.

9.7. The objective of Articles 5(1)(f) and 32(1) is to ensure that controllers and processors implement a level of security appropriate to the risk presented by their processing operations. Non-compliance with each of these provisions can have adverse impacts on the rights and freedoms of data subjects and must be dissuaded. Article 14 requires certain information to be provided to data subjects, and supplements the core data protection principles of fair and transparent processing.

9.8. I consider that the formal recognition of the seriousness of infringements by means of a reprimand is appropriate and necessary to ensure compliance with these Articles. A reprimand is proportionate in the circumstances where it does not exceed what is required to enforce compliance with the GDPR, taking into account the serious nature of the infringements and the potential for harm to data subjects.

9.9. In it submissions dated 6 June 2023 in response to the Revised Draft decision, the DOH stated the following:

> …the Department acknowledges and accepts the proposed reprimand in respect of our infringements of the GDPR which we duly recognise.[98]

B. Ban on processing

9.10. Article 58(2)(f) GDPR provides that a supervisory authority shall have the power to "*impose a temporary or definitive limitation including a ban on processing*."

9.11. In light of the findings contained herein that the DOH does not have a lawful basis to process certain personal data collected using the 2019 Template under Articles 6(1)(e), 6(4) or 9(1) of the GDPR, I impose a ban on the DOH processing the excessive personal data in Category A collected in response to questions 3 and 4 of the template in the 29 SENs litigation files examined for Purpose A.

9.12. I consider that this ban on is appropriate, necessary and proportionate in view of ensuring compliance with the infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR. This is additionally a further step to ensure that the DOH brings its processing into compliance with the GDPR.

[98] DOH's submissions, 6 June 2023, page 6

9.13. Considering this ban on processing, I do not consider it appropriate or necessary to impose a requirement on the DOH to update its transparency information, as it will no longer be permitted to process personal data for the purposes that were omitted from the description set out in the privacy notice examined. I also do not consider it necessary to impose orders in relation to the infringements of Articles 5(1)(f) or 32(1) GDPR considering the technical and organisational measures that were adopted by the DOH following the Temporal Scope of Issue C.

9.14. The DOH referred to the Data Sharing and Governance Act 2019 ('**2019 Act**') in its submissions, stating

> [92] Section 6 of the 2019 Act provides that, "Section 38 of the Data Protection Act 2018 shall not apply to the disclosure of information by one public body to another public body."
>
> [93] It does not appear that the implications of this legislative change were considered by the DPC in the Draft Decision. Insofar as the DPC proposes to consider the application (or non-application) of the 2019 Act in the final Decision, the Department requests an opportunity to be heard in relation thereto and reserves its entitlement to make a submission in relation to same.
>
> [94] In particular, while section 6(2) of the 2019 Act has not yet entered into force, when commenced, it will have implications for the corrective measures imposed by the DPC, and in particular on the DPC's proposal to impose "a ban on collecting further personal data" from the HSE using "any of the questions set out the 2019 Template".

9.15. First, it is unclear what reliance the DOH is seeking to place on section 6(2) of the 2019 Act. Section 38(1) of the 2018 Act is permissive, and allows controllers to process personal data necessary and proportionate for the performance of their functions. Section 6(2) of the 2019 Act, which was commenced on 16 December 2022, *disapplies* section 38(1) of the 2018 Act to data sharing between state bodies. As a result, while the DOH may have sought to rely on section 38(1) of the 2018 Act during the Temporal Scope to collect information from other public bodies, it can no longer do so because of the provisions of section 6(2) of the 2019 Act. I found above that the DOH could not rely on section 38(1) of the 2018 Act to process personal data for Purpose A. I made no finding of infringement or otherwise in relation to whether it could rely on section 38(1) for Purpose B. The fact that there is now a statutory prohibition on relying on this provision for data sharing between government departments would only underscore the finding of infringement, and would not result in a reversal of that finding. It would have no impact on the finding in relation to Purpose B.

9.16. More generally, section 6(1) of the 2019 Act states, "Subject to subsections (2) and (3), nothing in this Act shall affect the operation of data protection law." Since 7 July 2021, controllers must comply with the requirements of the 2019 Act regarding the putting in place of data sharing

agreements under Part 4 of the 2019 Act. In line with section 6(1) of the 2019 Act, these requirements are in addition to the obligations under data protection law, and do not affect the findings or corrective measures in this Decision.

9.17. In it submissions dated 6 June 2023 in response to the Revised Draft decision, the DOH stated the following:

> …the Department accepts the ban on the processing of personal data in the SEN litigation cases which has been confirmed as being neither necessary nor proportional for the purposes under which it was obtained. The Department accepts your position that the proposed ban on processing this excessive data is an additional step to ensure that the Department brings its processing into compliance with the GDPR.[99]

C. Administrative fine

9.18. In addition to the corrective powers under Articles 58(2)(b) and 58(2)(f), I have also decided that the DOH's infringements of Articles 5(1)(c), 6(1)(e), 6(4) and 9(1) GDPR warrant the imposition of an administrative fine. I have decided that the infringement of Article 14 GDPR does not warrant the imposition of a separate administrative fine for the reasons outlined in connection with Article 83(3) GDPR below. I have also determined that a reprimand is sufficient for the infringements of Articles 5(1)(f) and 32(1) GDPR.

i. <u>Whether each infringement warrants an administrative fine</u>

9.19. Article 58(2)(i) permits the DPC to consider the imposition of an administrative fine, pursuant to Article 83, in addition to, or instead of, the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in section 115 of the 2018 Act, which permits the DPC to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2). Article 83(1), in turn, identifies that the administration of fines "*shall in each individual case be effective, proportionate and dissuasive*." In this context, when deciding whether or not to impose administrative fines and the amount of any such fines, I must give due regard to the criteria set out in Article 83(2) GDPR, which provides that:

> Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
>
> (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

[99] DOH's Submissions 6 June 2023, page 7

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

9.20. These criteria are crucial to the decision as to whether or not to impose administrative fines and the amount of any such fines. Therefore, I will consider each of these criteria in turn in respect of the DOH's infringements GDPR.

9.21. In applying the Article 83(2)(a) to (k) factors to the infringements, I have set out below my analysis of the infringements collectively where it is possible to do so. However, in some instances it is necessary to set out each infringement individually in order to reflect the specific circumstances of each infringement and the factors falling for consideration. Regardless of whether the analysis below is individual or collective in respect of a particular factor or infringement, I have considered every infringement separately when deciding whether to impose an administrative fine in respect of each infringement. I have made a separate decision on each infringement, and I have made each decision without prejudice to any factors arising in respect of the other infringements. For the avoidance of doubt, my decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine where applicable, is independent and specific to the circumstances of each particular infringement.

a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

Issue A – Infringements of Articles 5(1)(c), 6(1)(e), 6(4) and 9(1) GDPR

9.22. I concluded that the DOH had breached Articles 6(1)(e), 6(4) and 9(1) GDPR in relation to Issues A, finding that the DOH did not have a legal basis to process personal data in Categories A and B(i) for Purpose A.

9.23. The nature of the DOH's infringements of Articles 6(1)(e), 6(4) and 9(1) GDPR comprises a failure to process personal data lawfully. Articles 6 and 9 set out legal bases for processing personal data, in the absence of which the processing is unlawful and amounts to an infringement of the fundamental right to data protection set out in Article 8 of the CFR and supplemented by the GDPR. The personal data was sought in relation to 21 open SENs litigation files, and its nature was inherently sensitive. It included special category data and other personal data that related to private aspects of the data subjects' lives. As such, the infringement of these provisions has the potential to result in damage or distress to data subjects.

9.24. The gravity of the infringements is serious in circumstances where the information had originally been obtained by the HSE and DOE for the purposes of providing services to data subjects, and the DOH did not have a valid legal basis to process the personal data for Purpose A. Moreover, as a government department, the DOH is in a position of power in the State. By contrast, the data subjects were vulnerable and the information that was provided by the HSE to the DOH had been obtained from them in circumstances where they had a reasonable expectation that it would be held in confidence. Therefore, the infringements are of an extremely grave nature.

9.25. Having regard to the Temporal Scope, the duration of the infringements was from 25 May 2018 to 29 March 2021. Therefore, the infringements are one year, 10 months and four days in duration.

9.26. The nature of the infringement of Article 5(1)(c) involved the collection and processing by the DOH of information in the absence of an assessment as to what was strictly necessary to process for Purpose A. The gravity of this infringement is particularly severe in the examples of the DOH receiving information directly from a hospital doctor. More generally, the infringement of Article 5(1)(c) is serious. That infringement involved the failure by the DOH to consider the necessity of the information in question for the purposes it pursued.

9.27. Having regard to the Temporal Scope, the duration of the infringements was from 25 May 2018 to 29 March 2021. Therefore, the infringements are one year, 10 months and four days in duration.

Issue B – Infringement of Article 14 GDPR

9.28. The nature of the infringement of Article 14 was that the DOH did not provide plaintiffs and other data subjects with information required under Article 14 GDPR. Article 14 supplements the principles of transparency and fair processing set out in Article 5(1)(a) GDPR, and allows data subjects to understand which of their personal data is processed by a controller and for what purposes.

9.29. The gravity of this breach is serious, as it led to data subjects being unaware of the manner in which their personal data were processed by the DOH. In particular, data subjects were unaware of the fact that state organisations were sharing information in the manner outlined herein.

9.30. Having regard to the Temporal Scope, the duration of the infringements was from 25 May 2018 to 29 March 2021. Therefore, the infringements are one year, 10 months and four days in duration.

b) the intentional or negligent character of the infringement;

9.31. The Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 provide that:

> In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.[100]

9.32. Those Guidelines proceed to detail how supervisory authorities should determine whether wilfulness or negligence was present in a particular case:

> The relevant considerations about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.[101]

9.33. In determining whether an infringement was intentional, I must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration. In determining whether an infringement was negligent, I must determine whether, despite there being no knowledge and wilfulness in respect of the characteristics of the infringement, the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

[100] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, WP 254, adopted on 3 October 2017, 11
[101] Ibid at page 12

9.34. The EDPB noted in its Binding Decision 2/2022 that:,

> [204] The EDPB recalls that the CJEU has established a high threshold in order to consider an act intentional. In fact, even in criminal proceedings the CJEU has acknowledged the existence of "serious negligence", rather than "intentionality" when "the person responsible commits a patent breach of the duty of care which he should have and could have complied with in view of his attributes, knowledge, abilities and individual situation" . In this regard, the EDPB confirms that a company for whom the processing of personal data is at the core of its business activities is expected to have sufficient measures in place for the safeguard of personal data: this does not, however, per se change the nature of the infringement from negligent to intentional.

9.35. The DOH made submissions in respect of these issues in its submissions of 9 March 2022. As noted by the EDPB in its Binding Decision 2/2022, "having knowledge of a specific matter does not necessarily imply having the "*will*" to reach a specific outcome."[102]

9.36. I do not consider that DOH acted wilfully with respect to the characteristics of the infringements of Articles 5(1)(c), 6(1), 6(4) or 9(1) GDPR. Therefore, I find that these infringements were not intentional.

9.37. However, I find that the infringements of those provisions were negligent. In making this finding, I have had regard to the resources available to a department of state. A department in the position of the DOH ought to have been aware of its obligations regarding data minimisation and the lawfulness of processing.

c) Any action taken by the controller or processor to mitigate the damage suffered by data subjects;

9.38. In its submissions, the DOH referred to a number of steps taken by it to mitigate the damage suffered by data subjects as a result of the infringements. These include:

- *additional controls have been put in place in relation to the storage of documents containing personal information;*
- *responsibilities in relation to the processing of personal information under the General Data Protection Regulation (GDPR) have been highlighted to all staff within the Department. A new Mandatory Data Protection Awareness Training Module has been developed and rolled out to staff and all staff have been reminded of their Data Protection responsibilities and,*
- *a Data Protection Impact Assessment (DPIA) of these litigation records has commenced*.

9.39. Considering that the DOH denies any infringement of Articles 5, 6 or 9 GDPR, no specific mitigating steps have been taken by the DOH in respect of the infringements identified in

[102] At paragraph 203

relation to subsections of those provisions. However, the training and DPIA outlined above are general mitigating steps that will be taken into account in respect of all of the infringements identified herein.

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

9.40. I consider that the DOH holds a high degree of responsibility for these failures. It did not take appropriate technical and organisational measures to ensure compliance with the provisions GDPR that it infringed. The organisational measures implemented by the DOH, including the 2019 Template, undermined the principle of data minimisation and the requirements to have a lawful basis for processing under Articles 6 and 9 GDPR. In those circumstances, the DOH did not implement appropriate technical and organisational measures to ensure data protection by design and default, in accordance with Article 25 GDPR.

9.41. As outlined above, the DOH also infringed Articles 5(1)(f) and 32(1) GDPR by failing to implement appropriate technical and organisational measures regarding its processing of personal data on its SENs litigation files. I consider that the DOH holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. However, in circumstances where this factor forms the basis for the finding of the infringements of Articles 5(1)(f) and 32(1) against the DOH, this factor cannot be considered aggravating in respect of those infringements.

e) any relevant previous infringements by the controller or processor;

9.42. There are no relevant previous infringements by the DOH.

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

9.43. The DOH has cooperated fully with the DPC in the context of the Inquiry, allowing the Inquiry Team to inspect its files in spite of the fact that it claims that a number of documents in the files in question attract LPP. As noted earlier, the DOH has put in place mitigating measures in order to remedy some of the infringements and mitigate their possible adverse effects.

g) the categories of personal data affected by the infringement;

9.44. The categories of personal data affected by all of the infringements included special categories of personal data. The personal data including data concerning health in the form of information received directly from a doctor in one case, and clinical and psychological reports in other instances.

9.45. I also consider that the categories of personal data affected by the infringements included personal data that was sensitive as it related to private aspects of the plaintiffs' lives. The personal data collected included data relating to family circumstances, and amounted to a

serious interference with the private and family life of the plaintiffs who have taken SENs litigation against the DOH.

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so and to what extent, the controller or processor notified the infringement;

9.46. The infringement became known to the DPC through the disclosures made by the Whistleblower to *Prime Time*. The DOH did not notify the infringements to the DPC. Thus, the circumstances of the infringement are such that an internal staff member felt it was necessary to make public disclosures regarding their nature.

9.47. The DOH does not appear to have conducted an assessment of the lawfulness of processing personal data received from the HSE or co-defendants in the context of SENs litigation in advance GDPR, and has not put in place appropriate technical and organisational measures in order to ensure compliance with a number of its obligations under the GDPR. In those circumstances, it did not take proper steps to ensure that it could become aware of infringements GDPR, and it led to a situation where a staff member considered it necessary to make protected disclosures in respect of the infringements. Those circumstances are considered aggravating for the purposes of the imposition of an administrative fine.

i) Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

9.48. Corrective powers have not previously been ordered against the DOH with regard to the subject-matter of this Decision.

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

9.49. There are no relevant applicable codes of conduct or approved certification mechanisms. Therefore, this factor is neither mitigating nor aggravating in the circumstances.

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

9.50. I consider that the matters considered under Article 83(2)(a) – (j) reflect an exhaustive account of both the aggravating and mitigating factors applicable in the circumstances of the case.

9.51. When imposing corrective measure(s), I am obliged to select the measure(s) that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures. The Administrative Fines Guidelines provide that:

> "*The assessment of what is effective proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either*

to re-establish compliance with the rules, or to punish unlawful behaviour (or both)." [103]

9.52. I find that an administrative fine is necessary and appropriate in respect of the infringements in providing an effective, proportionate and dissuasive response in the particular circumstances of this case and in order to effectively pursue the objective of re-establishing compliance with Articles 5(1)(c), 6(1)(e), 6(4) and 9(1) GDPR in respect of the subject matter of the processed discussed at Issue A.

9.53. In making this decision, I have had regard to the orders and reprimand made in this Decision. Those corrective powers are of utility in re-establishing compliance and in providing an effective and dissuasive response. I consider that the reprimand made is of significant value in dissuading future non-compliance. This formal recognition of the seriousness of the DOH's infringements is likely to contribute somewhat to ensuring an appropriate level of compliance with those provisions GDPR going forward. Furthermore, in regard to the ban on processing, I note that this order has significant value in re-establishing compliance with the provisions contained therein because it obliges the DOH to take certain specified steps in implementing technical and organisational measures.

9.54. However, having regard to the circumstances of the infringements of Articles 5(1)(c), 5(1)(e), 6(1)(e), 6(4) and 9(1) I find that the order and reprimand alone are not effective and proportionate in re-establishing compliance and in dissuading future non-compliance. Those articles place a continuous obligation on controllers to ensure that they have a lawful basis to process personal data, and a basis for processing special categories of personal data. Controllers must ensure that they can rely on at least one lawful basis in respect of any processing of personal data. This reflects a fundamental principle of data protection law, and the wording of the CFR. Article 5(1)(c) places a continuous obligation on controllers to process only the minimum amount of personal data necessary for their purposes. I do not consider that the reprimand alone constitutes a sufficiently effective, proportionate and dissuasive response to the infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) in light of the need to re-establish compliance and to dissuade non-compliance. In coming to the conclusion that an administrative fine is also necessary, I have particular regard to how personal data concerned were sensitive and included special categories of personal data. Furthermore, I have regard to the proportionality assessment carried out in relation to Issue A and the seriousness of the actions of the DOH with the infringements of fundamental rights under the CFR. I also have regard to the negligent nature of those infringements, and the imbalance in power between the DOH and the relevant data subjects. In light of those aspects of the infringements, I consider that an administrative fine is appropriate, necessary and proportionate to ensure compliance with of Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR.

[103] Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

9.55. I have had regard to all the corrective powers available to me as set out in Article 58(2) GDPR. For the reasons set out above, and having particular regard to the matters discussed under Article 83(2)(a)-(j) cumulatively, I consider it appropriate to impose an administrative fine in respect of the infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR in addition to the order and reprimand imposed in this Decision.

ii. The permitted range

9.56. Having decided that the infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR warrant the imposition of a fine, I must next proceed to decide on the amount of that fine. First, it is necessary to consider the appropriate cap for the fine as a matter of law. The cap determines the permitted range for the fine, from a range of zero, to the cap. However, the cap is not a starting point for a fine.

9.57. The permitted range for this administrative fine is set out in section 141(4) of the 2018 Act.[104] The fine shall not exceed €1,000,000 because the DOH is a public authority[105] that does not act as an 'undertaking' within the meaning of the Competition Act 2002.[106]

iii. Calculating the administrative fine

9.58. The Revised Draft Decision set out a proposed range for the administrative fine and the factors to be considered when calculating the fine in order to provide the DOH with the opportunity to comment in accordance with fair procedures. As a matter of European law, it is settled jurisprudence in respect of the calculation of fines that the body imposing the fine should not anticipate the submissions of parties by providing the final proposed fine in its statement of objections.[107] In applying this principle, it is impossible to specify a precise figure without having regard to the views of the party subject to the Inquiry. Moreover, it is clear, as a matter of Irish

[104] Section 141(4) provides: "Where the Commission decides to impose an administrative fine on a controller or processor that— (a) is a public authority or a public body, but (b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002, the amount of the administrative fine concerned shall not exceed €1,000,000."

[105] Public authority is defined in section 2 of the 2018 Act as including "any other person established by or under an enactment (other than the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act)". The DOH was established pursuant to S.I. No. 58/1947 – Health (Transfer of Departmental Administration and Ministerial Functions) Order, 1947

[105] Section 2 of the Ministers and Secretaries (Amendment) Act 1946v.I. No. 58/1947 – Health (Transfer of Departmental Administration and Ministerial Functions) Order, 1947

[105] Section 2 of the Ministers and Secretaries (Amendment) Act 1946 and, thus, is a public authority within the meaning of the 2018 Act.

[106] Undertaking is defined in section 3 of the Competition Act 2002 as "a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of a service". As the DOH does not provide its services for a gain, it is not an undertaking within the meaning of that Act.

[107] Cases 125/2007 P, 133/2007 P, 135/2007 P and 137/2007 *P Erste Group Bank v Commission* (ECLI:EU:C:2009:576), [182]

law, that the DOH is entitled to be informed of the allegations against it and given the opportunity to respond. [108] On this basis, I set out below the method of calculating the fine, the factors to be taken into account and the final amount of the administrative fine.

9.59. In the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology.[109] The methodology that I have followed is intended to set out clearly and unequivocally the elements taken into account in calculating the fine, having allowed the DOH, as the addressee, to understand the basis for the fine and ensuring that the fine is calculated in a rational manner.

9.60. The methodology that I followed in calculating the administrative fine is as follows. The first step in calculating the administrative fine is to consider the permitted range and to determine a final amount for the fine within that permitted range. In this regard, the cap provided for in section 141(4) of the 2018 Act is not the starting point for the fine. Rather, it is relevant to determining the permitted range. The determination of where on the permitted range the appropriate fine lies is made by reference to the nature, gravity, and duration of each infringement, as considered in relation to Article 83(2)(a) above, and the other mitigating and aggravating factors. The determination is made in the context of the objectives of re-establishing compliance, including through deterrence, and to provide a proportionate response to the unlawful behaviour. Then it considers whether the figure arrived at is "*effective, proportionate and dissuasive*" in the circumstances in accordance with Article 83(1) GDPR.

iv. Total value of administrative fine(s)

9.61. Article 83(3) GDPR states:

> '*If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*.'

9.62. In a recent decision, the EDPB held that the reference to 'gravest infringement' in Article 83(3) did not relate to gravest infringement identified in a particular inquiry, but rather referred to the fining caps referred to in Articles 83(4) and Article 83(5) GDPR.[110] Accordingly, as Decision Maker I am not restricted to only imposing administrative fines for the most serious infringement GDPR in this case. Thus, where the legislator has provided for distinct requirements in the form of separate legislative provisions, separate fines can be stipulated.

[108] *Gunn v Bord an Choláiste Náisiúnta Ealaíne is Deartha* [1990] 2 IR 168, 179

[109] See by analogy *Electrabel v Commission*, T 332/09, ECLI:EU:T:2012:672, [228], *Marine Harvest ASA v Commission*, T-704/14, ECLI:EU:T:2017:753, [450]

[110] Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (Adopted on 28th July 2021).

9.63. However, as noted above in the conclusion in Issue B, I consider that there was an overlap between the infringement identified in that section and the infringement identified in Issue A. The failure to provide information to data subjects about the DOH's practices was fundamentally linked with the unlawfulness of its processing for Purpose A – the primary reason why the DOH did not provide information to data subjects was to avoid the reactivation of litigation. Bearing in mind the principle of *ne bis in idem*, I do not consider that it is appropriate to impose a separate fine for the infringement of Issue B.

9.64. In locating the fine on the permitted range of €0 to €1,000,000, I have had regard to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the intentional character of the infringements as assessed in accordance with Article 83(2)(b) above, the responsibility of the controller as assessed in accordance with Article 83(2)(d) and the sensitivity of the categories of personal data in accordance with Article 83(2)(g). I have also had regard to the mitigating factors outlined in accordance with Articles 83(2)(c) and 83(2)(f).

v. <u>The final amount for the administrative fine</u>

9.65. Based on the analysis above, I found, in the Revised Draft Decision, that the range for the administrative fine of infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) would be between €15,000 to €30,000. This is reduced from a potential range of €17,000 to €43,000 in the Draft Decision, to take account of the fact that I have removed one of the findings of infringement for which a fine was proposed to be imposed in the Draft Decision.

9.66. The final step is to consider whether the figure arrived at is "*effective proportionate and dissuasive*" in the circumstances in accordance with Article 83(1) GDPR. I find that a final amount of €22,500 meets these requirements. In order for any fine to be effective, it must reflect the circumstances of the individual case. As outlined above, the infringements of Articles 5(1)(c), 6(1), 6(4) and 9(1) are serious. This fine takes account of the sensitive nature of the personal data, and the fact that some of it had been obtained in circumstances of doctor-patient confidentiality. It also takes account of the respective positions of the DOH and the data subjects by virtue of their statuses as a state department and individuals in receipt of services for special educational needs.

9.67. In order for a fine to be dissuasive, it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. I am satisfied that the amount of €22,500 is dissuasive to both the DOH and similar controllers. As regards the requirements for any fine to be proportionate, this requires me to adjust the quantum of any fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that amount of the fine does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringements on the data subject rights enshrined in the GDPR and also taking into account the fact that the DOH is a state body with control over the provision of health

services in the state. Accordingly I am satisfied that amount of the fine above would be effective, proportionate and dissuasive, taking into account all of the circumstances of the Inquiry.

9.68. In it submissions dated 6 June 2023 in response to the Revised Draft decision, the DOH stated the following:

> …with some reservation, in terms of the proposed range of the administrative fine, pursuant to Article 83, in respect of the Department's admitted infringements of the GDPR, the Department accepts the provisionally proposed measure. The Department acknowledges the fairness of the proposed decision of a fine in the range of €15,000 to €30,000, not least when noting the maximum fine which could be applied to a public body as a corrective power. The Department is however mindful that this punitive measure while deemed necessary, will ultimately be met with funds provided to the Department from the public purse, and we would consequently appreciate leniency in this proposed corrective measure, when your final decision is concluded.[111]

9.69. Based on the analysis of Issue A I have set out above, and taking into account the DOH's final submissions and the fact that they have accepted the findings and corrective measures, I impose the following administrative fine:

- In respect of the DOH's infringement of Articles 5(1)(c), 6(1), 6(4) and 9(1), I impose a fine of €22,500.

E. Summary of Corrective Powers

9.70. By way of summary, this Decision proposes to impose the following corrective action:

- An ban on processing in the terms outlined in Part 9B of this Decision;
- A reprimand; and
- A fine of €22,500.

10. Right of Appeal

10.1. This Decision is issued in accordance with section 111 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, the DOH will have the right to appeal against the final Decision within 28 days from the date on which notice of the Decision is received by it. Furthermore, as this Decision includes a decision to impose an administrative fine, pursuant to section 142 of the 2018 Act, the DOH will also have the right to appeal against the decision to impose an administrative fine within 28 days from the date on which notice of the Decision is given to it.

[111] DOH's Submissions, 6 June 2023, page 7

Helen Dixon

Commissioner for Data Protection

Appendix: Schedule of Materials Considered for the Purposes of this Decision

1. *RTÉ Investigates: The Department, The Data & The Disclosure* (Thursday 25 March 2021) Source: RTÉ Player (RTÉ Investigates: The Department, The Data & The Disclosure - RTÉ Player (rte.ie)) accessed 10 November 2021
2. Notice of Commencement of Inquiry 29 March 2021
3. Notification of Inspection Letter 29 March 2021
4. Letter dated 1st April 2021 from Secretary General, Department of Health to DPC.
5. Department of Health Document: "AP01 Description of Legal Approach to Special Education Needs Cases"
6. 2017 Template used by the Department of Health to obtain service updates from the HSE
7. 2019 Template used by the Department of Health to obtain service updates from the HSE
8. Note of Interview of Whistleblower by DPC 5 May 2021
9. Chain of Emails re File No. XXX
10. Letter dated 3rd August 2017 from the Office of the Attorney General to the Department of Health re "Transfer of Clinical Information in Special Education Needs Cases"
11. Internal Department of Health files collected by the Case Officers during the Inquiry
12. Inquiry Issues Paper
13. Submissions dated 4 October, 2021 of the Department of Health on Inquiry Issues Paper and cover letter.
14. Department of Health, Report to the Secretary General : "Review conducted to establish the facts with regard to the set of allegations made by RTE Prime Time Programme regarding Special Education Needs ("SEN") Litigation" Published 21st April 2021
15. Preliminary Screening/Assessment Report (In the matter of the Protected Disclosures Act 2014) 9 November 2020.
16. Draft Decision of DPC in the matter of the Dept of Health, reference IN-21-3-2
17. Submissions of the DOH to the DPC of 9 March 2022
18. Letter from the DPC to the DOH of 11 August 2022
19. Letter from the DOH to the DPC of 14 October 2022
20. Revised Draft Decision of DPC in the matter of the Dept of Health, reference IN-21-3-2
21. Submissions of the DOH to the DPC of 6 June 2023