



THE COURT OF APPEAL - UNAPPROVED

Court Of Appeal Record Number: 2023/282

High Court Record Number: 2022/191JR

Neutral Citation Number: [2024] IECA 152

**Noonan J.
Ní Raifeartaigh J.
Binchy J.**

BETWEEN/

JOHNNY RYAN

**APPLICANT /
APPELLANT**

- AND -

DATA PROTECTION COMMISSION

RESPONDENT

- AND -

(BY ORDER) GOOGLE IRELAND LIMITED

NOTICE PARTY

JUDGMENT of Mr. Justice Binchy delivered on the 24th day of June 2024

1. This is an appeal from a decision of the High Court whereby Simons J. refused the application of the appellant for a declaration that the respondent has failed to carry out an investigation into a complaint lodged by the appellant pursuant to the provisions of article 77 of Regulation (EU) 2016/679 (General Data Protection Regulation) (“the GDPR”) with all due diligence, and further refused the application of the appellant for an order of

mandamus directing the respondent to proceed with the investigation of that part of the complaint which the appellant claims the respondent has refused to handle. While I set out in detail below the circumstances in which the dispute between the parties has arisen, the issue that falls for determination is whether it is permissible for the respondent to defer the investigation of one element of a complaint in circumstances where all other elements of the same complaint are the subject of an inquiry – called for by the same complainant – being conducted by the respondent pursuant to s. 110 of the Data Protection Act, 2018 (the “2018 Act”), the outcome of which (it is said) may render it unnecessary to determine that element of the complaint, the consideration of which the respondent has deferred. In posing the question thus, it is necessary to observe immediately that there is disagreement between the parties as to the scope of the inquiry upon which the respondent has embarked, and this disagreement is explained and considered in detail later in this judgment.

2. The appellant in these proceedings is a senior fellow with the Irish Council for Civil Liberties. The respondent is the supervisory authority in the State established for the purposes of the GDPR, in accordance with article 51 thereof.

3. Before proceeding to consider the background to the proceedings, it is useful to identify now the relevant legislative provisions as well as some relevant authorities in which those provisions have been considered, and upon which reliance has been placed by the parties.

Relevant Provisions of the GDPR

4. Recital 141 of the GDPR provides:-

“Every data subject [defined as an identified or identifiable natural person] should have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that

his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period.”

5. Article 77 of the GDPR provides that every “data subject” shall have the right to lodge a complaint with a supervisory authority in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. The respondent is the supervisory authority in this jurisdiction for the purpose of the GDPR.
6. Article 78 provides data subjects with the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. This includes the right to a remedy where a supervisory authority does not handle a complaint, or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to article 77.
7. Article 57(1)(f) requires the supervisory authority to handle complaints lodged by a data subject and to “*investigate, to the extent appropriate [my emphasis], the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period...*”.
8. Article 5 of the GDPR is entitled “*Principles relating to processing of personal data*”. Three provisions of article 5 are relevant for present purposes, those being articles 5(1)(a), (c) and (f). Those provisions provide that personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
- (c) adequate relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
- (f) 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 (“integrity and confidentiality”)

9. Article 6 of the GDPR, entitled “*Lawfulness of processing*” sets out the circumstances in which the processing of data is deemed lawful by the GDPR. Article 32 of the GDPR, entitled “*Security of processing*” addresses the obligation of data controllers and data processors to ensure a level of security of data appropriate to the risks involved as referred to therein.

Relevant Authorities of the CJEU

10. It has been held (and stated repeatedly) by the Court of Justice of the European Union (the “CJEU”) that supervisory authorities have an obligation to handle complaints with all due diligence. In Case C-311/18, *Schrems II*, EU:C:2020:559, at para. 112, the CJEU held:-

“Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.”

11. At the time that these proceedings came on for hearing before the High Court, there was pending before the CJEU the Joined Cases of C-26/22 and C-64/22 *UF and AB v. Land Hessen and Schufa Holding AG*, EU:C:2023:222. The High Court judge had available to

him the opinion of Advocate General Pikamäe upon which he placed some reliance. While the CJEU has since given judgment in those cases, the principles discussed by the Advocate General and relied upon by the High Court judge in these proceedings remain relevant. At paras. 37 - 46 of his opinion, the Advocate General considered the role of supervisory authorities, including their obligation to examine complaints. He said, *inter alia*:-

“38. The Court has ruled that under [Article 57(1)(f) GDPR] ‘each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of the [GDPR], any data subject is entitled to lodge It should be pointed out in this connection that the Court has underlined the supervisory authority’s obligation to ‘handle such a complaint with all due diligence’ in order to ensure compliance with the provisions of the GDPR. It should also be noted that recital 141 of the GDPR states that ‘the investigation following a complaint should be carried out ... to the extent that is appropriate in the specific case’

39. All these factors suggest that the supervisory authority has a binding obligation to handle complaints lodged by data subjects with all due diligence that is appropriate in the specific case. In so far as any infringement of the GDPR is, in principle, capable of constituting an infringement of fundamental rights, it would seem to be incompatible with the system established by that regulation to allow the supervisory authority discretion as to whether or not to handle complaints. Such an approach would undermine the crucial role conferred on it by the GDPR

...

41. Although the supervisory authority, as guarantor of compliance with the provisions of the GDPR, is required to handle complaints lodged with it, several factors militate in favour of an interpretation to the effect that it enjoys a margin of assessment in examining those complaints and a degree of latitude in the choice of the appropriate

means to carry out its tasks. Advocate General Saugmandsgaard Øe has noted that Article 58(1) of the GDPR ‘confers on the supervisory authorities ... significant investigative powers’ and that they have, under Article 58(2) of that regulation, ‘a wide range of means ... of carrying out the task entrusted to [them]’”

12. So far as is relevant to these proceedings, *Hessen* was concerned with a question as to whether article 78(1) of the GDPR must be interpreted as meaning that judicial review of a decision on a complaint taken by a supervisory authority is limited to the question of whether that authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, or whether that decision is subject to a full judicial review, including the power of the court seized to require the supervisory authority to take a specific measure. The court determined that the latter interpretation is correct i.e. the decision of the supervisory authority is subject to a full judicial review. At para. 62 of its judgment, the court held:-

“If Article 78(1) of [GDPR] were to be interpreted as meaning that the judicial review referred to therein is limited to verifying whether the supervisory authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, the attainment of the objectives and the pursuit of the purpose of the regulation would necessarily be compromised.”

Data Protection Act, 2018 (the “2018 Act”)

13. The 2018 Act was enacted for the purpose of giving further effect to the GDPR. Part VI, Chapter 2 of the 2018 Act deals with enforcement of the GDPR. Section 108 deals with complaints, and under s. 108(2) the respondent is obliged to handle complaints in respect of which it is the competent supervisory authority. Section 109(1) imposes an obligation on the respondent to *“examine the complaint and ... in accordance with this section, take such*

action in respect of it as the Commission, having regard to the nature and circumstances of the complaint, considers appropriate.”

14. Section 110 empowers the respondent to conduct inquiries, *inter alia*, into complaints or of its own volition.

Background to the Proceedings

15. On 12th September 2018, solicitors acting on behalf of the appellant, using the online complaint form of the respondent, submitted a complaint on behalf of the appellant claiming that parties identified therein, including the notice party, were, in the course of their commercial activities, acting in continuous violation of the GDPR. Detailed particulars of the complaint were set out in a document attached to the form entitled “Grounds of Complaint to the Data Protection Commissioner” (the “Grounds of Complaint”) as well as in another document referred to in the complaint, authored by the appellant and referred to as the “Ryan Report”. While there is some dispute between the parties as to whether or not the documentation submitted by the appellant on 12th September 2018 constituted a complaint for the purposes of the GDPR, or the 2018 Act, that is not an issue in these proceedings. As a matter of expedience therefore, and without wishing to express any view on that issue, I will refer to the documentation submitted by the appellant on 12th September 2018 as the “Complaint”.

16. The Complaint is concerned with what is described as the “behavioural advertising” industry and, more specifically, what is described as “real time bidding” (“RTB”). It is stated that there are two systems of RTB, the first being described as “Open RTB” and, the second, and more relevant for present purposes, being the system operated by the notice party known as “Authorised Buyers”. It is said that both systems operate to provide personalised advertising on websites. At para. 5 of the Grounds of Complaint, the appellant identifies what he describes as “*three key, related causes for significant concern*”. These are:

- (i) The gathering of a wide range of information on individuals, far beyond what is required to provide relevant advertisements, and the provision of that information to a host of third parties for purposes well beyond those which a data subject can understand or consent or object to.
- (ii) The [RTB] mechanism does not enable the industry to control the dissemination of personal information once it has been broadcast. The personal data is not secure once broadcast to third parties, and therefore, data breaches are inherent in the design of the industry.
- (iii) Thirdly, data gathered and disseminated will very often include special category data indicating matters such as the ethnicity, political opinions and sexual orientation of data subjects. Since the data are likely to be disseminated to numerous organisations who would seek to amalgamate data received with other data, intricate profiles of data subjects may be produced without their knowledge or consent.

17. Two entities were identified by the appellant in the Complaint as being involved in the operation of the practices described. Firstly, IAB Europe, which is described as a trade association that sets parameters and design for use. While the appellant made complaints within the proceedings about the manner in which the respondent addressed the Complaint so far as concerns IAB Europe, those complaints are no longer relevant mainly because issues concerning IAB Europe were addressed by the supervising authority in Belgium, where that entity has its headquarters. The second entity whose practices have given rise to the Complaint is the notice party.

18. In the Grounds of Complaint, it is asserted that a number of the data protection principles set out in article 5 GDPR are engaged. Specifically, the appellant asserted breaches of articles 5(1)(a), (c) and (f) of the GDPR.

19. At para. 25 of the Grounds of Complaint, it is stated: “*Our principal concern is that the current frameworks and policies relating to the industry fail to provide adequate protections against unauthorised, and potentially unlimited, disclosure and processing of personal data*”. On 19th June 2019, the solicitors for the appellant provided additional information to the respondent. In a covering email, the appellant’s solicitors addressed what they claimed was the scale of the problem. They claimed that within the RTB system (at that time) there were 2,033 companies involved in advertising exchanges of personal data of which it appears 833 “*serve and measure ads to users in the EEA*”. It is claimed that there appears to be no control on information passing from those 833 companies operating within the EEA to the remaining 1,200 odd companies operating outside the EEA. They stated that given the volume of information sharing, and the speed and frequency at which it takes place, the system cannot comply with article 5(1)(f) GDPR.

20. In the Grounds of Complaint, the appellant invited the respondent to consider his submissions as a complaint pursuant to s. 119 of the 2018 Act. The appellant further invited the respondent to commence an inquiry pursuant to s. 110 of the 2018 Act, and in particular to conduct an investigation into the wider practices of the industry.

21. It should be noted that the Complaint as initially made by the appellant related to systemic practices within the online advertising industry, and he did not claim at this point that there had been any violation of his personal data. That complaint came later, on 2nd September 2019, when the appellant submitted evidence to the respondent that his personal data had been processed in the course of the notice party’s RTB mechanism.

22. In the meantime, i.e. between the initial filing of the Complaint in September 2018, and the provision of information by the appellant regarding the processing of his personal data in September 2019, there had been much correspondence between the parties, as well as a meeting between the parties that took place on 15th February 2019. On 22nd May 2019,

the respondent commenced the inquiry which the appellant had requested (the “Inquiry”). This is an inquiry pursuant to s. 110 (1) of the 2018 Act, and is known as an “own volition inquiry”. Section 110(1) provides as follows:-

“The Commission, whether for the purposes of section 109(5)(e), section 113(2), or of its own volition, may, in order to ascertain whether an infringement has occurred or is occurring, cause such inquiry as it thinks fit to be conducted for that purpose.”

23. The appellant provided further information and evidence regarding the processing of his personal data on 6th December 2019. In this correspondence, the solicitors for the appellant requested confirmation that the respondent was treating the appellant’s case as a complaint under article 77 of the GDPR and s. 108 of the 2018 Act.

24. By letter dated 22nd January 2020, the respondent confirmed to the appellant’s solicitors that the appellant’s case was being treated as a complaint within the meaning of s. 107 and for the purposes of s. 108 of the 2018 Act. In the same letter, the appellant was informed that in view of the fact that the respondent was examining matters in the context of the Inquiry which may substantially overlap with and influence the outcome of the Complaint, the respondent would handle the Complaint in line with and based upon the progress of the Inquiry. This led to the respondent having an inquiry and a complaint into substantially the same issues, although the extent of the overlap is disputed, and the difference between the parties on this issue is of importance.

25. On 18th February 2020, the appellant’s solicitors wrote to the respondent, *inter alia*, raising further queries as to the status of the Complaint. On 29th May 2020, the respondent sent two letters to the appellant’s solicitors in reply to these queries. One letter, sent by a Ms. Harrison, a solicitor and assistant commissioner in the office of the respondent, addressed matters relating to the Inquiry, and the other letter, sent by a Mr. Dougan, assistant commissioner, addressed the Complaint.

26. In the course of her letter, Ms. Harrison addressed the scope of the Inquiry as follows:-

“In terms of its current scope, the Inquiry is examining the following issues:

- (i) Whether Google has a lawful basis for processing of personal data, including special category data, for the purposes of targeted advertising via the Authorised Buyers mechanism and, specifically, for the sourcing, sharing and combining of the personal data collected by Google with other companies/partners;*
- (ii) How Google complies with its transparency obligations, particularly with regard to Art. 5(1), 12, 13 and 14 of the GDPR;*
- (iii) The legal basis/bases for Google’s retention of personal data processed in the context of the Authorised Buyers mechanism and how it complies with Article 5(1)(c) in respect of its retention of personal data processed through the Authorised Buyers mechanism.”*

27. It is immediately apparent that the scope of the Inquiry does not include the complaint that Google’s activities are in breach of article 5(1)(f) of the GDPR. The reference to article 5(1) within para. (ii) clearly could not be a reference to article 5(1)(f) because of its reference to transparency rather than integrity and confidentiality.

28. In his letter, Mr. Dougan, reiterated what had been said in the letter of 22nd January 2020 about the overlap between the issues in the Inquiry and the issues in the Complaint. He said that since the outcome of the Inquiry may inform the handling of the Complaint, or elements of the Complaint, it was the intention of the respondent in the first instance to progress the Inquiry. The appellant’s solicitors addressed this in a reply of 7th August 2020 to the respondent.

29. As with much of the correspondence exchanged between the parties, the letter of 7th August 2020 from the appellant’s solicitors to the respondent is a long letter addressing multiples issues arising out of both the Inquiry and the Complaint. So far as is relevant to

these proceedings, however, and specifically to article 5(1)(f) GDPR, the appellant's solicitors stated that: "*...whilst the DPC has conducted an 'own volition' inquiry in response to our client's complaint, that inquiry does not cover all ground raised in our client's complaint. In particular, the Inquiry date (sic) does not address Article 5 (1)(f) of the GDPR. Our client's complaint has not therefore been substantively progressed since it was first lodged with the Data Protection Commission in September 2018, twenty-two months ago.*"

Later in the same letter the appellant's solicitors requested that, since the Inquiry does not address article 5(1)(f) GDPR, that the respondent consider the infringement of that article as an additional consideration to those being considered by the respondent in the "Own Volition Inquiry".

30. The respondent replied by letter of 7th September 2020. By way of response to the appellant's complaint that the respondent was not considering the complaint of an infringement of article 5(1)(f), the respondent referred to the reasons given by the appellant in the Grounds of Complaint for his opinion that the notice party's authorised buyers guidelines operate in breach of article 5(1)(f). In this regard, the appellant had complained, at para. 27 of the Grounds of Complaint, that the authorised buyers guidelines do not:

- (a) Require notification to data subjects of the dissemination of their data or of any intention or decision to broadcast their data to every recipient;
- (b) Afford individuals an opportunity to make representations to vendors/recipients of data in respect of how their personal data may be used;
- (c) Grant a formal right to data subjects to object to the use of their data by those individual third parties; and
- (d) Provide for any, or any sufficient, control to prevent unlawful and/or authorised further usage.

31. Paragraph 27 of the Grounds of Complaint appears under the heading: “*Integrity and confidentiality*”. In its letter of 7th September 2020 to the appellant’s solicitors, the respondent, at para. 3.3 states (as regards the particulars given in para. 27):-

“The Commission, having considered these concerns in the course of its consideration of the scope of the Inquiry, was of the view that, rather than engaging, specifically, issues of data security which is the essence of the obligation under Article 5(1)(f), these issues were more closely aligned to the issues of transparency and lawfulness of processing. However, the Commission continues to have an open mind in relation to the central matters which fall for consideration in this Inquiry.

In this regard, it is not the intention of the Commission to exclude from the scope of the Inquiry any areas of potential systemic risk to data subjects. The Commission has, under s. 110(1), discretion to scope the Inquiry as it sees fit, and in this context, it continues to keep the scope of the Inquiry under review.

As set out below, the Commission is presently awaiting receipt of further submissions from Google. Following its receipt and consideration of Google’s further submissions, and once the full factual matrix has been established, the Commission may, at that time, consider it appropriate to revisit the scope of the Inquiry to include the examination of other provisions of the GDPR. As set out below at paragraph 5.2, your client will, in due course, be provided by the Commission with an issues paper, which will set out, in more detail scope of the Inquiry and the issues being examined as part of the same.”

32. In a letter of 23rd December 2021, the solicitors acting on behalf of the appellant addressed this issue as follows:-

“15 months have passed since your reply of 7 September 2020 and yet our client is still unaware if his concerns in relation to Article 5(1)(f) are being addressed in the context of the Own Volition Inquiry or not.

If it is the case that his concerns in relation to Article 5(1)(f) are not being addressed in the context of the Own Volition Inquiry, it must follow that they must be investigated in the context of the Complaint Based Inquiry. There is no lawful reason, bearing in mind your duty to investigate complaints with ‘all due diligence’, that the investigation relating to the alleged breaches of Article 5(1)(f) is not proceeding in either the Own Volition Inquiry or the Complaint Based Inquiry. Put simply, if you have not extended the scope of the Own Volition Inquiry to include our client’s concerns in relation to Article 5(1)(f), you have a duty to proceed on the investigation of that aspect of our client’s complaint in the Complaint Based Inquiry. You cannot suspend the Complaint Based Inquiry on the basis that the Own Volition Inquiry addresses the issues raised in the Complaint Based Inquiry if, on its face, the Own Volition Inquiry does not extend to include certain issues raised in the complaint.”

33. In a further reply of 12th January 2022, the respondent reiterated that, for the purposes of the own volition Inquiry, it was of the view that the central issues requiring determination are those relating to transparency, the legal basis, data minimisation and storage limitation, to the exclusion of any issue relating to data security. The respondent stressed that it had no difficulty in saying that, when resuming examination of the Complaint, it would consider again whether issues relating to data security should be the subject of scrutiny in that context. The respondent expressed the view that, when considering such matters, it would need to have regard to the contents of the Brave Report (another name for the Ryan Report) and the report submitted by the appellant in September 2019, because in the view of the respondent, only limited reference was made to article 5(1)(f) in those documents, and the appellant’s

reliance upon that provision was described as “*recent*”. It was stated that the respondent might need to consider whether or not the appellant’s more recent emphasis on article 5(1)(f) involves a re-casting and/or expansion of the complaint.

34. The appellant’s solicitors replied by further letter of 14th January 2022, and described the respondent’s approach as “*astonishing*”. They asserted that the data security issue had been described from the very outset as being the “*principal concern*” of the appellant. They repeated their call that the respondent should investigate the issue of data security within the context of the Complaint, since the issue has been excluded by the respondent from the Inquiry.

35. In the course of the correspondence that followed, it became apparent that the respondent’s interpretation of the Complaint so far as concerns article 5(1)(f) is different to the interpretation of the appellant. In a letter of 27th January 2022, the respondent expressed the view that the point being made by the appellant in the Complaint was not that the *security* of the RTB systems may be compromised, or is susceptible to unauthorised access or disclosure of personal data in what the respondent described as a “*narrow sense*”, but rather that the appellant’s complaint was that, structurally, the systems are built on processing operations some or all of which are incompatible with the requirement that personal data be processed lawfully. For this reason, the respondent directed its attention to questions as to whether or not those processing operations have a legal basis by reference to articles 5(1)(a) and 6 of the GDPR. The respondent observed that article 5(1)(f) also makes reference to “*unauthorised and unlawful processing*”, and that the appellant had not sought to engage with article 32 GDPR, which addresses security of processing by data controllers and processors. The respondent expressed the view that, in circumstances where security, *per se*, is not the focus of the various submissions made by the appellant to the respondent, there is little or nothing of substance between the parties in relation to the Complaint. The

respondent contended that the appellant had been aware since 29th of May 2020 that the Inquiry will be progressed in the first instance in circumstances where the outcome of the Inquiry may have a bearing on the Complaint, and the point was made that if, for example, at the conclusion of the Inquiry the respondent found that the processing operations that are central to the RTB systems do not in fact have a legal basis, then it is reasonable to anticipate that the respondent would require such operations to cease.

36. In a reply dated 31st January 2022, the solicitors for the appellant asserted that the respondent misunderstands the Complaint, and stated that the appellant's complaint is precisely that the security of the RTB systems may be compromised, or are susceptible to unauthorised access or disclosure of personal data in the narrow sense described by the respondent. It was stated that the appellant's complaint is not confined to arguments that, structurally, the systems are built on processing operations some or all of which are incompatible with the requirement that personal data be processed lawfully. It was stated that the security of the RTB systems has always been the principal concern of the appellant. The appellant's solicitors concluded: "*As we have now clarified any confusion in respect of the complaint's scope, we invite you to confirm by close of business on Wednesday 2 February 2022 that you will immediately investigate the complaint as it pertains to Art. 5(1)(f) data security issues*", and further stated that if such confirmation was not forthcoming within that timeframe, then proceedings would issue.

37. Notwithstanding the deadline, further correspondence on the difference of interpretation of the Complaint ensued, without resolution, although the respondent at all times made it plain that it remains open, in principle, to considering the Complaint in the context of article 5(1)(f) following upon the conclusion of the Inquiry. The final position of the appellant on the issue was put forward in a letter from his solicitors of 15th February 2022 as follows:-

“Moreover, the DPC’s contention that the structural flaws inherent in Google’s system ‘can most effectively be addressed otherwise than by means of Article 5(1)(f)’ are misplaced. For instance, the focus on transparency and lawfulness will not address the ‘primary concern’ of our client’s complaint. Even if the legal basis for processing could be regularised, that will not resolve the security issues pertaining to the uncontrolled broadcast of personal data as that broadcast will continue unabated. Simply, Google’s system does not have ‘appropriate security’. That lack of security leads to ‘unauthorised’ processing in the meaning of 5(1)(f). The inherent lack of security in Google’s RTB broadcast of personal data is, and always has been, the primary focus of the Complaint. The DPC acknowledged this as a central concern in their initial acknowledgement of the Complaint. The DPC must therefore investigate the continued and ongoing breaches of Article 5(1)(f) with all due diligence, regardless of the outcome of the investigation into the other issues raised by the Complaint/Own Volition Inquiry.”

38. In the course of this letter, the appellant’s solicitors asserted that the approach of the respondent was inconsistent with that adopted by the Belgian supervisory authority in its investigation of IAB Europe. They claimed that the Belgian authority had examined whether or not IAB Europe’s processing activities infringed article 5(1)(f) and had identified a lack of security within IAB Europe’s transparency and consent framework such as to render that system untenable, and those conclusions would apply *mutatis mutandis* to the notice party’s authorised buyers RTB system.

39. The respondent replied by letter dated 28th February 2022, this being the last letter sent prior to the institution of proceedings. This letter was sent by a Mr. Kevin Kennedy, solicitor. In this letter, Mr. Kennedy reiterates the respondent’s reasons as to why it was not considered

necessary to investigate, for the time being, the allegation of an infringement of article 5(1)(f), stating as follows:-

“There is a very simple reason why, to date, Article 5(1)(f) has not been central to the DPC’s consideration of your clients complaint, i.e. the complaint (which we would reiterate is concerned with the processing of your client’s personal data), does not allege that your clients personal data has been the subject of manipulation of the kind with which the Belgian DPA was concerned. That being so, it is entirely rational that our consideration of the complaint would proceed by reference to the structure of the underlying processing system and, further, that where the structure of that system is already the subject of scrutiny in our Own-Volition Inquiry, we would look to close out the Own-Volition inquiry first in sequence. In that regard, and has been explained, at length, and repeatedly, the structure of the underlying scheme is being examined in the context of the Own-Volition Inquiry by reference to the issues of legal basis and transparency, being the same approach taken by the Belgian DPA.

For completeness, we wish to make it clear that we fundamentally disagree with the contention made in your letter that findings adverse to the controller in relation to the issue of legal basis “will not resolve the security issues pertaining to the uncontrolled broadcast of personal data....”

That contention is wrong.”

The Proceedings

40. On 14th March 2022 of the appellant applied for and obtained leave to issue proceedings by way of judicial review seeking, *inter alia*, the following reliefs:

- (i) A declaration that the respondent has failed to carry out an investigation into the Complaint... with all due diligence and/or within a reasonable period, as required by article 57 GDPR and/or the 2018 Act.

- (ii) An order of *mandamus* directing the respondent to proceed with the investigation of that part of the Complaint not addressed in the Inquiry... without delay and with all due diligence.
- (iii) Insofar as it may be necessary for the determination of the within proceedings, a reference to the Court of Justice of the European Union, pursuant to article 267 of the Treaty on the Functioning of the European Union.

41. The grounds upon which the reliefs are sought may be succinctly stated. The appellant claims that the respondent is obliged to carry out an investigation into each of the issues raised in a complaint which in this instance includes a complaint relating to breaches of article 5(1)(f) GDPR. Where the respondent chooses to investigate those complaints in the context of an own-volition inquiry, it remains under an obligation, *inter alia*, to progress that inquiry – or at least those parts relating to the complaint – within a reasonable period and with all due diligence, and to provide the complainant with updates every three months. Where the respondent is not addressing those complaints in the Inquiry, it is obliged to investigate them separately, without delay, within a reasonable period and with all due diligence. Therefore, in the circumstances of this case, the refusal of the respondent to investigate the alleged breaches of article 5(1)(f) GDPR, whether in a timely manner, or at all, constitutes a clear breach of its obligations under, *inter alia*, article 77 GDPR and/or the 2018 Act.

42. Insofar as the respondent has claimed that, by addressing other aspects of the Complaint, it might address the concerns of the appellant in relation to article 5(1)(f), this is not correct. The respondent is under an obligation to investigate the entirety of the Complaint. In the event that the respondent were to find the appellant's complaint to be made out, the extent of the offending behaviour of the notice party is relevant to

consideration of the appropriate measures or sanctions to be imposed upon the notice party by the respondent.

43. In its statement of opposition, the respondent pleads that it has at all times consistently maintained that it will progress and conclude the Inquiry before considering the Complaint as the Inquiry has the potential to resolve or substantially narrow the issues raised in the Complaint. Moreover, it is pleaded that the respondent has made it clear in correspondence that it is open to engaging with any issues in relation to article 5(1)(f) GDPR in the context of the Complaint, while maintaining that such issues as the appellant raises in respect of article 5(1)(f) GDPR are in substance the same issues which fall to be examined in the Inquiry. In the circumstances, it is pleaded that the appellant's claim that issues relating to data security have not been considered by the respondent is premature.

44. It is further pleaded that where the respondent decides to initiate an "own-volition" inquiry pursuant to the provisions of s. 110(1) of the 2018 Act, it has a discretion to determine the scope of such inquiry. It is further pleaded that the respondent is entitled to deploy its financial resources in a manner it considers most appropriate, having regard to its statutory functions and obligations.

Judgment of the High Court

45. Simons J. delivered judgment on 28th August 2023. At para. 32 thereof, he observed that the appellant does not seek to challenge the respondent's decision as to the scope of the own volition inquiry, and nor does he challenge the pace of the progression of the Inquiry. Rather, the appellant's challenge is directed exclusively to the procedural decision to defer the consideration of the appellant's complaint pending the completion of the Inquiry.

46. The trial judge summarised the appellant's argument at para. 29 in the following terms (and it should be observed that the appellant agrees with this summary):-

“29. The Applicant submits that there is an obligation, as a matter of EU law, on the Commission qua supervisory authority to proceed with the handling of a complaint with all due diligence. This obligation is said to entail a duty to investigate fully any complaint that the individual’s data protection rights have been infringed. It is said that the Commission is under a duty to take action on a complaint and is not entitled to defer investigation. On this argument, not only is the Commission precluded from deferring consideration of a complaint pending the completion of an inquiry the Commission would not even be allowed to determine individual issues within a complaint on a modularised or sequenced basis.”

47. At para. 31, the trial judge noted that the appellant accepts that it would have been lawful for the respondent to “hive off” all issues raised in a complaint to the respondent, and then to defer the investigation of the complaint pending the conclusion of such an inquiry. Accordingly, the appellant’s objection is that the complaint of an infringement of article 5(1)(f) is not being considered as part of the Inquiry, and for that reason the appellant maintains that this issue should be investigated now or in parallel with the Inquiry.

48. The key conclusions of the High Court are to be found at paras. 33 - 35 in which Simons J. concluded as follows:-

“33. The absolutist position advocated for by the Applicant is too extreme. It is incorrect to say that a supervisory authority cannot defer consideration of a complaint pending the completion of related investigations or inquiries. This is especially so where, as in the present case, the data processing operations the subject of the complaint are under active investigation in the own-volition inquiry, albeit not by reference to all of the legal heads asserted by the Applicant.

34. It is apparent from the language of the GDPR that a margin of appreciation is afforded to a supervisory authority. In particular, the obligation to investigate a

*complaint is couched in qualified terms, i.e. to investigate, to the extent appropriate, the subject matter of the complaint. As observed by Advocate General Pikamäe in the passages from *UF v. Land Hessen* cited earlier, the supervisory authority enjoys a margin of assessment in examining complaints and a degree of latitude in the choice of the appropriate means to carry out its tasks. This must include discretion as to the sequencing of investigations and inquiries. The extent of the investigation which is appropriate in the case of a particular complaint will often depend on the outcome of related inquiries and investigations which are already ongoing as of the date the complaint is lodged.*

35. In deciding on the extent to which it is appropriate to investigate a complaint, the supervisory authority is entitled to weigh factors such as, inter alia, the seriousness or gravity of the alleged infringement; the need to marshal its resources so as to prioritise investigations appropriately and the need to comply with fair procedures for all sides, including those parties who are the subject of the investigation.”

49. The trial judge then proceeded to consider the margin of appreciation enjoyed by the respondent in the handling of the complaints. At paras. 39 - 40 the trial judge concluded as follows:-

“39. Here, the Commission has taken a decision to defer consideration of one aspect of the Applicant’s complaint pending the completion of its own-volition inquiry. This does not amount to a refusal to investigate the complaint, still less a refusal to handle the complaint. Rather, it is a sequencing decision. The substance of the complaint overlaps, to a significant extent, with the issues being investigated in the own-volition inquiry. The Commission has kept the Applicant fully apprised of the reasons for its sequencing decision and of the progress of the own-volition inquiry. The Commission has engaged in extensive correspondence with the Applicant on these matters.

40. The decision to prioritise the own-volition inquiry is proportionate and well within the margin of appreciation allowed to a supervisory authority. The Commission is engaged on a complex and time-consuming inquiry into the behavioural advertising industry. It is entirely proportionate for the Commission to have decided to complete the own-volition inquiry first, before completing its investigation of the Applicant's complaint."

50. The judge noted that the respondent had made the point that if the Inquiry results in a determination that the processing operations of the notice party do not have a legal basis, then the respondent would have to consider imposing a ban on their further operation, although the appellant contended that an adverse finding on the issue of lawfulness will not resolve the security issues raised by the appellant in the Complaint.

51. The judge also took into account that the respondent had also received a number of complaints from other data subjects, which are based on the same report as that relied upon by the appellant and therefore raise the same systemic issues. Moreover, so far as issues of security are concerned, they have been raised in the context in which the RTB systems are structured i.e. whereby personal data may, *by design*, pass beyond the control of the controller, and are not concerned with accidental loss, destruction or damage, and the Inquiry is already addressing the structural framework through an examination of the lawfulness and transparency of the notice party's processing operations. For these reasons, the judge observed, the respondent was of the view that its approach of dealing with the number of systemic issues as part of the own-volition inquiry in the first instance is the most efficient and consistent way of dealing with such issues and subsequent, individual complaints which relate to the same. In the view of the High Court judge, the respondent had articulated a clear rationale for its procedural decision to prioritise the own-volition inquiry over the Complaint and that the overall approach of the respondent is appropriate and proportionate.

52. The judge also noted that the Inquiry has reached the point of a preliminary draft decision, in relation to which the appellant and the notice party will have the opportunity to make submissions. He also took into account that the respondent has “*consistently explained to the Applicant that it remains open to addressing the alleged breach of Article 5(1)(f) in the context of its consideration of his complaint.*” (para. 47).

53. Finally, in the interests of completeness, and not least because it has given rise to a ground of appeal, I should mention that the judge considered the standard of review applicable to decisions of the respondent. In this context, he noted that the court must determine whether the respondent has exceeded the margin of appreciation afforded to it under the GDPR. He said that in light of the observations of Advocate General Pikamäe, it is arguable that the standard of review under GDPR is more searching than that of unreasonableness or uncertainty per *O’Keeffe v. An Bord Pleanála* [1993] 1.I.R. 39 and may approximate more closely to that applicable in the case of a statutory appeal, i.e. the threshold of serious or significant error. He referred to *Nowak v. Data Protection Commissioner* [2016] IESC 18, [2016] 2 I.R. 585. But he concluded that he did not have to resolve the issue because whichever test applied, the test of serious or significant error or the higher test of proportionality, the “*procedural decision*” made by the respondent passes muster.

The Appeal

54. While there are six grounds of appeal, the central ground of appeal pursued at the hearing is that the High Court judge erred in determining that the respondent’s decision to defer consideration of the appellant’s complaints of breaches of article 5(1)(f) (including its consideration of whether to investigate such complaints) pending completion of the own volition inquiry was lawful. In particular, it is said that the High Court judge failed to apply properly the provisions of the GDPR and the relevant judgments of the CJEU, in particular Case C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650 and Case

C-311/18, *The Data Protection Commissioner v. Facebook Ireland Limited*,
ECLI:EU:C:2020:559.

55. In his second ground of appeal, it is claimed that the judge erred in applying the principle of curial deference under Irish law to the failure and/or refusal of the respondent to investigate the entirety of the appellant's complaint with all due diligence, as required by European law.

56. By his third ground of appeal, the appellant claims that the High Court judge erred in failing to consider the effect of a refusal to investigate/deferral of investigation of part of the appellant's complaint, which is not otherwise been handled or investigated by the respondent.

57. By his fourth ground of appeal the appellant claims that the High Court judge erred in finding that the respondent had kept the appellant fully apprised of the reasons for its sequencing decision and the progress of the own-volition enquiry.

58. The fifth ground of appeal concerns a procedural matter which was not pursued, and the sixth ground of appeal is that the High Court judge erred in awarding the respondent its costs of the proceedings.

Submissions

59. It is the appellant's case that the issues raised by the proceedings have significant consequences for his data protection rights, and that the respondent, as the designated supervisory authority, has an obligation under article 51 GDPR to protect those rights. The appellant refers to article 57(f) of the GDPR, which obliges supervisory authorities to "*handle complaints lodged by a data subject... and investigate to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period....*"

60. It is submitted that the phrase “*to the extent appropriate*” is illuminated by recital 129 of the GDPR which provides:-

“The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular 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, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned....”

61. In *Schrems II* in the context of considering the obligations of supervising authorities under article 58(2)(f) of the GDPR, in circumstances where data was intended to be transferred to a third country where the protections provided by EU law are not provided, the CJEU said at paras. 109 and 112:-

“109. In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required in its territory to handle complaints which in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence....

...

112. Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is

nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.”

62. The appellant contends that the respondent’s letter of 12th January 2022 makes it clear that the appellant’s complaint under article 5(1)(f) is not going to be investigated in the course of the Inquiry, and that it might never be investigated, even after the conclusion of the Inquiry. The appellant characterises the treatment of the article 5(1)(f) complaint in the letter of 12th January 2022 as a refusal on the part of the respondent to investigate a core element of the appellant’s complaint.

63. Furthermore, the appellant contends that, contrary to the assertions of the respondent, there is no overlap between the matters under investigation in the Inquiry on the one hand and the Complaint on the other, as regards breaches of article 5(1)(f). Accordingly, regardless as to whatever conclusions the respondent may reach in the Inquiry regarding breaches of articles 5(1)(a), (c) and/or (e) the respondent will not have reached any conclusions on the alleged breaches of article 5(1)(f). Therefore, by the conclusion of the Inquiry, the alleged breaches of article 5(1)(f) will not have been investigated, handled or progressed at all, let alone with any due diligence.

64. It is submitted that the High Court judge erred in rejecting the appellant’s arguments that the opinion of the Advocate General in *Hessen* was authority for the proposition that the respondent was required to investigate breaches of article 5(1)(f) without delay or suspension, and that the subsequent judgment of the CJEU further endorses the principles in *Schrems I* and *Schrems II*, that investigations must be carried out with all due diligence, which cannot include suspension of the investigation itself.

65. It is submitted that while Advocate General Pikamäe found that supervisory authorities enjoy discretion in the investigation of complaints, he did not make any finding that modularisation or sequencing of investigations is permissible, and it is submitted that such

discretion as supervisory authorities enjoy is not unlimited, and remains subject to the principles underlying the GDPR, including the obligation to investigate complaints with all due diligence. The appellant further argues that the suspension of an investigation of a specified, identified breach of the GDPR, which is not being progressed at all for reasons unrelated to that breach, cannot vindicate the rights of the appellant as required under the GDPR per the CJEU in *Hessen*.

66. In its written submissions, the appellant contended that the High Court judge erred in considering that the higher standard of review – that of serious or significant error – might apply to decisions of the respondent. It was submitted that such an approach would be inconsistent with the decision of the CJEU in *Hessen* in which it was stated that: “... *the requirement for effective judicial protection would not be met if decisions concerning the exercise by such a supervisory authority of powers of investigation or the adoption of corrective measures were subject only to limited judicial review.*”

67. Finally, it is submitted that the High Court judge erred in finding that the appellant was “*kept fully informed*” by the respondent. The appellant submits that there was a failure to make it clear to the appellant that the article 5(1)(f) complaint was not being investigated by the respondent since at least April 2021, and perhaps earlier.

Submissions of Respondent

68. The respondent argues that it has never refused to handle or investigate the Complaint, and that it has stated unequivocally that it will “*resume examination of the complaint as soon as a decision is issued in relation to the own-volition inquiry*”. This, it is submitted, was made clear in the respondent’s letter to the appellant’s solicitors of 27th January 2022.

69. The respondent submits that the High Court judge was correct in concluding that the respondent has simply sequenced its investigation procedures in order to prioritise the resolution of an extremely complex and resource intensive industry wide inquiry ahead of

an investigation of the appellant's individual complaint, due to the significant overlap between the issues arising in the Inquiry and the substance of the Complaint.

70. Furthermore, the respondent has provided a clearly reasoned rationale for sequencing the Inquiry ahead of the Complaint, and has kept the appellant informed as to the progress of the Inquiry and has involved the appellant in the Inquiry as an interested person whom the respondent has permitted to make submissions in the particular circumstances.

71. It is submitted that as a supervisory authority under the GDPR, the respondent enjoys a broad margin of appreciation in the conduct of its statutory tasks, including the examination of complaints, and that the manner in which it has sequenced its investigations fall well within its margin of appreciation, as was found by the High Court judge.

72. The respondent submits that the appellant has failed to explain why the handling of complaints with "*all due diligence*" mandates the *immediate* investigation of *all* aspects of a complaint, even where a supervisory authority has formed a reasonable and *bona fide* view that the most efficient allocation of its resources justifies the prioritisation of a related inquiry ahead of a complaint, with a review of what may be left of the complaint to be considered thereafter. The respondent submits that the arguments of the appellant ignore the clear recognition of the CJEU of the margin of discretion resting with the supervisory authority as to "*choice of appropriate and necessary means*" regarding how it deals with the complaint [per *Hessen*, para. 68].

73. The respondent submits that the High Court judge made key factual findings or drew inferences from the affidavit evidence in respect of which the appellant has failed to engage in any meaningful analysis. In particular, the judge found that the respondent had not refused to investigate the breaches of article 5(1)(f) of the GDPR as was submitted by the appellant. Secondly, the judge found that the respondent has explained to the appellant its reasoned

basis for temporarily deferring the Complaint, and has kept the appellant fully apprised of its approach and the progress of the Inquiry.

74. It is submitted that the appellant bears the burden of demonstrating that the judge was incorrect in arriving at these findings of fact. In this regard, the respondent relies upon *Blythe v. Commissioner of An Garda Siochána* [2023] IECA 255, at para. 47 and also the judgment of Charleton J. in *Ryanair Limited v. Billigfluege.de GmbH* [2015] IESC 11.

75. The respondent submits that while the appellant has relied upon the general statements of the CJEU regarding the requirement to handle complaints with “*all due diligence*”, the appellant has failed to explain how the respondent is not observing that requirement in the conduct of the Inquiry and the handling of the Complaint.

76. The respondent submits that the decision of the CJEU in *Hessen* is not of direct relevance insofar as it is concerned with the standard of review to be applied to a legally binding decision of a supervisory authority, and not the manner in which a supervisory authority decides to handle a complaint in the first place. Even so, however, the respondent submits that the opinion of Advocate General Pikamäe is supportive of the respondent’s case insofar as he opined that “*several factors militate in favour of an interpretation to the effect that a [supervisory authority] enjoys a margin of assessment in examining those complaints and a degree of latitude in the choice of appropriate means to carry out its tasks.*” While acknowledging that Advocate General Pikamäe stated that a supervisory authority does not have a discretion as to whether or not to handle complaints, the position in this case is that the respondent has not refused to handle the Complaint but instead is exercising the degree of latitude that it enjoys in the carrying out of its tasks by deferring the investigation of the Complaint until the conclusion of the Inquiry.

77. The respondent submits that there is nothing at all in the authorities, *Schrems I*, *Schrems II* or *Hessen* that establishes that a supervisory authority may not decide to defer

investigation of a complaint in an appropriate case. In this case, the appellant ignores the fact that the Inquiry – which is highly complex – has been actively progressed at all times.

78. The respondent also places some reliance upon the decision of the Court of Appeal in England and Wales in *Dalo v. Information Commissioner* [2023] EWCA Civ 1141, and also the decision of the Upper Tribunal in the case of *Killock v. Information Commissioner* [2022] 1 WLR 2241. However, the Court was not addressed in any detail about the extent of any differences between the provisions of the relevant legislation in the United Kingdom and the GDPR, and I am reluctant to have regard to those authorities without either an agreed position between the parties in this regard, or submissions on the extent and import of such differences as there may be between the two legislative regimes.

Discussion and Decision

79. The obligation of supervisory authorities such as the respondent to handle complaints with “*all due diligence*” is well established. It is obvious from the phrase itself that it affords supervisory authorities a measure of discretion in their handling of complaints, but this is in any event made clear by several provisions of the GDPR, such as recital 141 and article 57, each of which speak of the handling and investigation of a complaint “*to the extent appropriate*”, and also recital 129 which states that measures adopted by supervisory authorities in the exercise of their powers “*should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned*”.

80. In his opinion in the *Land Hesse*, Advocate General Pikamäe, having emphasised the binding obligation of supervisory authorities to handle complaints lodged by data subjects with the due diligence that “*is appropriate to the specific case*” (my emphasis), also stated

that “*several factors militate in favour of an interpretation to the effect that [supervisory authorities] enjoy a margin of assessment in examining those complaints and a degree of latitude and the choice of the appropriate means to carry out its tasks.*” In expressing this opinion, be relied upon the opinion of Advocate General Saugmandsgaard Øe in *Data Protection Commissioner v. Facebook Ireland Ltd (Case C-311/18) (Schrems II)*.

81. However, Advocate General Pikamäe made it clear that this discretion or degree of latitude does not include a discretion as to whether or not to handle complaints. That obligation is absolute. This is made very clear in para. 39 of the opinion of the Advocate General, where he says: “*[I]n so far as any infringement of the GDPR is, in principle, capable of constituting an infringement of fundamental rights, it would seem to be incompatible with the system established by that regulation to allow the supervisory authority discretion as to whether or not to handle complaints. Such an approach would undermine the crucial role conferred on it by the GDPR.*”

82. In this case, the appellant argues that the effect of the decision of the respondent to defer consideration of the Complaint until the conclusion of the Inquiry is to defer it *sine die*, and that this amounts to a refusal to handle the complaint. In any event, and however it is characterised, the appellant’s case is that the decision to defer the handling of the Complaint is not in compliance with the obligation to handle complaints with all due diligence. In considering this, it is important to bear in mind that the appellant’s objection relates to one element of the Complaint, that being his complaint under article 5(1)(f), having regard to the fact that all other elements of the Complaint are being addressed in the Inquiry. The respondent, however, maintains that in substance, all elements of the Complaint are under consideration in the Inquiry, and that it has agreed in any event to address such issues of data security as may not be addressed by the Inquiry, upon its conclusion, in the context

in which they were raised by the appellant, and having regard to the documents submitted by the appellant in support of the Complaint (see para. 33 above).

83. The appellant strongly disagrees that all elements of the Complaint are being addressed in the course of the Inquiry. As I mentioned above, the appellant argued that that the suspension of an investigation of a specified, identified breach of the GDPR (i.e the alleged infringement of article 5(1)(f) of the GDPR), which is not being progressed at all for reasons that he claims are unrelated to that breach, cannot be a vindication of the appellant's rights under the GDPR. This argument led to some debate at the hearing of this appeal about the extent of the overlap between the subject matter of the Inquiry and the complaint made by the appellant as to infringement of article 5(1)(f). The issue was also the subject of correspondence between the parties, as to whether the appellant by his complaint was referring to security in the broad or narrow sense (see paras. 35 and 36 above). In this regard, the observations of the High Court judge at para. 44 of his judgment are instructive:-

“The Commission makes the point that the security considerations raised by the complaint are not those typically arising under Article 5(1)(f) and Article 32 of the GDPR. The complaint is concerned with the way in which the real-time bidding systems are structured, i.e. whereby personal data may, by design, pass beyond the control of the controller, rather than concerned with accidental loss, destruction or damage. The own-volition enquiry is already addressing the structural framework through an examination of the lawfulness and transparency of Google's processing operations, i.e. the extent of the data subjects' knowledge of the processing, their control over that processing and the exercise of the rights.”

84. It is not entirely clear if the judge accepted this point, but he certainly did not reject it. The passage appears amidst a series of paragraphs in the judgment in which the judge summarises the rationale for the decision of the respondent to defer consideration of the

Complaint, and the judge clearly finds the rationale persuasive. In any case the point that is made – that personal data may, *by design*, pass beyond the control of the controller – appears to be reflected in the description of the operation of the authorised buyers guideline, within the Grounds of Complaint, where at page 9, para. 20 it is stated: “*This passage suggests that once the personal data is transferred to a Buyer, Authorized Buyer has no effective control over how that data is used. Rather, it is accepted that the third party (the Buyer) is free and able to utilise that data.*”

85. What all of this demonstrates is that the concerns advanced by the appellant under the heading of security, and which he wants investigated in the Complaint, are not typical security concerns; they relate to processing operations through which data is inevitably transferred by the notice party, *by design*, rather than technical issues such as the systems deployed to avoid unauthorised dissemination of data. These processing operations are, as the judge observed, the subject of investigation in the Inquiry under the headings of lawfulness and transparency rather than security. It follows that there is a very significant overlap between the matters under investigation in the Inquiry, and those identified by the appellant in the Complaint, even if they are being investigated by reference to a different provision of the GDPR.

86. Secondly in this regard, it is instructive to look at para. 27 of the Grounds of Complaint. It is here that the appellant himself explained why the notice party’s Guidelines do not provide adequate integrity and confidentiality in their data processing operations. The appellant provided four reasons. They were considered by the respondent, who formed the view that these reasons “*rather than engaging, specifically, issues of data security which is the essence of the obligation under Article 5(1)(f), [these issues] were more closely aligned to the issues of transparency and lawfulness of processing.*” This was explained by Ms. Harrison in her letter of 7th September 2020 to the appellant’s solicitors. I do not believe the

appellant's solicitors ever took issue with this analysis in correspondence. While the reasons are set out at para. 30 above, I will set them out again here as a matter of convenience:

[Google's Guidelines] do not:

- (a) require notification to data subjects of dissemination of their data or of any intention or decision to broadcast their data to every recipient.
- (b) afford individuals an opportunity to make representations to vendors/recipients of data in respect of how their personal data may be used.
- (c) grant a formal right to data subjects to object to their use of their data by those individual third parties. And,
- (d) provide for any, or any sufficient, control to prevent unlawful and/or unauthorised further usage.

87. In my view the characterisation of at least the first three of these reasons as being "*more closely aligned to the issues of transparency and lawfulness of processing*" was perfectly reasonable. That being so, this lends further support to the proposition that there is a very significant overlap between the issues under consideration in the Inquiry and those raised by the Complaint.

88. Finally under this heading, it is also instructive to consider the three matters identified by the appellant at the outset of the Grounds of Complaint as being "*key causes of concern*". These are set out at para. 16 above. In my estimation, these reasons are also more closely aligned with issues of transparency, lawfulness and data minimisation than with issues related to appropriate security as referred to in article 5(1)(f).

89. What is, I hope, demonstrated by the foregoing analysis is that, contrary to what was submitted by the appellant, there is indeed a substantial overlap between the subject matter of the Complaint (as regards the concerns articulated by the appellant under the heading of data security) and the investigations being undertaken in the course of the Inquiry under the

headings of lawfulness, transparency and data minimisation, such as to amount to a reasonable basis to defer the handling of the Complaint pending the outcome of the Inquiry.

90. There is also another reason why this is so. This is that if the processing operations are found (in the Inquiry) to have no legal basis, then the respondent would very likely require cessation of the operations. While the appellant says that a finding of unlawfulness could readily be addressed by the notice party (for example, by changing its consent procedures), the fact is that one possible outcome of the Inquiry would be such as to render the appellant's Complaint entirely moot.

91. The decision of the respondent to order matters as it has is, as the High Court judge found, quite clearly a "*sequencing decision*", and is one made against a background where, as I have found, the Inquiry is investigating substantially the same subject matter of the Complaint, notwithstanding that the extent of the overlap between the two is in dispute. I agree with the High Court judge that the respondent must be entitled to order the sequence in which it addresses the individual elements of a complex, multi-dimensional complaint, and to have regard to the fact that it is inquiring into the issues raised by the Complaint in the course of the Inquiry, even if there is not an exact overlap between the two. Moreover, as the judge also found, the respondent has kept the appellant fully apprised of the reasons for its sequencing decision and of the progress of the Inquiry, and, importantly, it has made it plain that upon the conclusion of the Inquiry it will investigate any elements of the Complaint that have not been considered in the Inquiry. I also agree with the judge that this manner of addressing the Complaint is proportionate and well within the margin of appreciation allowed to a supervisory authority.

92. It is true that the Inquiry is taking a long time, but the appellant is not making the case that the Inquiry is taking an unreasonable time. While the appellant appears to be of the view that that is so, he has not sought to rely on the point, and, wisely so in my opinion. The

time that the Inquiry is taking must be seen against the background of its undisputed complexity and the appellant's own description of RTB as involving "*the world's biggest data breach*". I make no comment on that, but repeat the description only to give a flavour of the scale of the task posed by the Inquiry.

93. For all of the foregoing reasons, I can find no error in the conclusion of the High Court judge that the decision of the appellant to prioritise the Inquiry and defer the handling of the Complaint is proportionate, and well within the margin of appreciation allowed to a supervisory authority. That conclusion disposes of the appellant's first, and main ground of appeal.

94. As to the appellant's second ground of appeal, whereby it is asserted that the judge erred in applying the standard of deference applicable to decisions of statutory bodies, this was not pursued at the hearing of this appeal, and I think wisely so. It is apparent from the judgment under appeal that the judge did not do so. He considered that whatever standard was applied, whether that of serious or significant error or the higher test of proportionality, the decision made by the respondent "*passes muster*", and I agree.

95. While grounds three and four of the grounds of appeal were addressed briefly in written submissions, they were not pursued in oral submissions to the Court. I will, however, address them briefly. Ground of appeal number three is that the High Court erred in failing to consider the effect upon the appellant of not investigating or deferring the investigation of the Complaint. This is not correct. The High Court did so, briefly, at para. 30 of the judgment, where the judge referred to the appellant's concerns that his personal data is being processed in a manner that does not ensure appropriate security of the data, in breach of article 5(1)(f) of the GDPR. It follows that the judge was aware of these concerns when conducting his subsequent analysis of the appellant's case. Moreover, the judge, in reaching

his conclusions, took into account that the respondent had explained that it remains open to addressing what remains of the Complaint, following upon the conclusion of the Inquiry.

96. The fourth ground of appeal is that the High Court erred in finding that the appellant was kept fully informed by the respondent. In his written submissions the appellant contends that this finding flies in the face of the correspondence, which it is submitted shows a lack of specificity and detail in communications from the respondent, and a failure to inform the appellant until December 2021 that the respondent had not been investigating article 5(1)(f) breaches since at least April 2021, and perhaps earlier.

97. This ground is not made out. All one has to do to see this is refer to the correspondence exchanged between the parties between 29th May and 7th August 2020, referred to at paras. 28 and 29 above. In any event, even if the ground of appeal was made out, it could not result in the granting of the declaratory and injunctive reliefs sought in the proceedings.

98. Ground five relates to the form of proceedings. It was not pursued at all. This related to the form of proceedings. For future reference, however, I think it worthwhile to refer to paras. 17-21 of the judgment of the High Court, where the judge pointed out that the reliefs sought should have been sought by way of an application under sub-sections 150(7) and (8) of the 2018 Act, rather than by way of judicial review. In the particular circumstances, however, he was prepared to overlook this procedural irregularity which he found to be of no consequence.

99. The proceedings shall next be listed on 28th June at 2.00pm in order to receive the parties' submissions on costs and to make final orders.