



Neutral Citation Number: [2021] EWHC 1427 (QB)

Case No: QB-2020-002788

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
MEDIA AND COMMUNICATIONS LIST

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 28/05/2021

Before :

THE HONOURABLE MRS JUSTICE COLLINS RICE

Between :

MR BALDO SANSÓ RONDÓN

Claimant/
Respondent

- and -

LEXISNEXIS RISK SOLUTIONS UK LIMITED

Defendant/
Applicant

Mr Hugh Tomlinson QC & Mr Aidan Wills (instructed by Schillings International LLP) for
the **Claimant**

Miss Lorna Skinner QC (instructed by Osborne Clarke LLP) for the **Defendant**

Hearing date: 20th April 2021

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this
Judgment and that copies of this version as handed down may be treated as authentic.

.....

Approved Judgment

Mrs Justice Collins Rice :

Introduction

1. The parties dispute a point of interpretation of the General Data Protection Regulation (GDPR). On the Defendant's interpretation, the Claimant has (in effect) tried to sue the wrong person and this litigation should end in its present form. On the Claimant's interpretation, his underlying claim proceeds, with time for filing and serving a defence starting to run in accordance with an extant case management Order.

The Underlying Claim

2. The Claimant, Mr Sansó Rondón, is a businessman with an international practice in business consultancy and investment. He holds Italian and Venezuelan citizenship. He is resident in Italy.
3. World Compliance Inc ('WorldCo') is a US company. It owns (and is the 'data controller' of) a database which it says is designed to help subscribing businesses globally to comply with laws combating money laundering and terrorism financing. The database includes millions of profiles of individuals, among them the Claimant. The Claimant objects to this profile, in the successive versions in which it has been published. He considers that WorldCo has not respected his rights under the GDPR.
4. The Defendant is a data analytics, risk intelligence and compliance business, incorporated in England and Wales. It is WorldCo's formally designated 'representative' for the purposes of the GDPR (Article 27).
5. The Claimant issued a claim against the Defendant in August 2020. The claim particularises a number of alleged breaches of the GDPR in WorldCo's processing of the Claimant's personal data, in producing the profile to which he objects. The particulars of claim assert that, as WorldCo's representative, the Defendant "*is liable in respect of breaches of the GDPR for which World Compliance Inc is liable as data controller*".
6. The remedies sought by this claim include:
 - (1) a compliance order under Section 167 of the Data Protection Act 2018 requiring the Defendant to erase (or cause to be erased) the Claimant's personal data, and restraining the Defendant from further unlawful processing of the Claimant's personal data;
 - (2) an order under Article 19 of the GDPR that
 - (a) the Defendant notify (or cause to be notified) each recipient to whom the Claimant's personal data have been disclosed, through their having accessed any version of the profile, of such erasure, and

Approved Judgment

- (b) the Defendant provide the Claimant with details of the identities of the recipients;
- (3) compensation pursuant to Article 82 of the GDPR.

The Defendant's Application for a Terminating Ruling

7. The Defendant applies for this claim to be struck out (under CPR Rule 3.4) or alternatively for summary judgment to be entered in its favour (under CPR Part 24). It says there are no reasonable grounds for bringing the claim, or alternatively the claim has no realistic prospect of success, because it is brought against the wrong defendant. It says a representative cannot be held liable for the actions of a controller as proposed, and the remedies sought can be obtained only from a controller, not its representative.
8. There is much about this application the parties agree on. They agree it turns entirely on the interpretation of what the GDPR says about the role and functions of Art.27 representatives. They agree no relevant guidance is provided on that by UK or EU decided caselaw. They agree there is a limited amount of potentially relevant assistance from other sources, as set out below.
9. They agree no fact-sensitive issues are raised, and nothing about the facts and circumstances of this particular case affects my task or should incline me to defer the question for consideration at trial – and there is no other good reason to do so. They agree, in other words, that the answer to the interpretative question is determinative of this application, and that a ruling is needed on a pure question of law.

Article 27 GDPR

10. Art.27 provides as follows:

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
2. The obligation laid down in paragraph 1 shall not apply to:
 - (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

Approved Judgment

- (b) a public authority or body.
3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
 4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.
 5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.
11. Art.27 is predicated on the application of Art.3.2. Art.3 provides for the territorial scope of the GDPR. It states:
 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union.
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
 3. ...
12. These provisions contain a number of defined terms – including concepts which have become the familiar building blocks of data protection law. These are explained in the definitional provisions of Article 4 GDPR. Art.4(17) makes a defined term out of the provision made by Art.27. It states:

‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Approved Judgment

13. The GDPR, read together with the Data Protection Act 2018, forms the data protection law of England and Wales. The GDPR originally took effect in the UK as directly-effective EU law (Regulation 2016/679) during the UK's membership of the EU. It continues in force through the 'retained EU law' provisions of the Brexit legislative regime. The parties do not suggest there is anything in the EU origins or Brexit history of the GDPR of *general* relevance or assistance in approaching the interpretative task. Some specific issues are considered below.

The Rival Interpretations of Article 27

14. The parties agree that the GDPR in general, and Art.3.2 and Art.27 in particular, apply in this case. The dispute between them is, in particular, as to the effects of Art.27.4 and Art.27.5.
15. The Defendant says the key, or sole, operative provision defining the role and functions of a representative is the phrase '*to be addressed*' in Art.27.4. That means what it says. A representative is a point of contact for those most closely interested in data protection compliance by foreign controllers: national 'supervisory authorities' or regulators (here, the Information Commissioner's Office (ICO)) and data subjects themselves. It is a liaison or conduit function. But a representative can no more be sued in place of a data controller than a legal adviser in place of a client. That, the Defendant says, is shown by Art.27.5: the designation of a representative is *without prejudice to* (has nothing to do with) the initiation of legal actions against the controller itself. It is also apparent from the wider scheme of the GDPR.
16. The Claimant says 'representative' means what it says: Art.4(17) underscores '*represents*'. Art.27.4 requires the *mandation* of a representative to be addressed *in addition to or instead of* the controller *on all issues* related to data processing and, importantly, *for the purposes of ensuring compliance with the GDPR*. Art.27.2(a) makes even clearer that the function of a mandated representative is to address the *risk to the rights and freedoms* of data subjects. None of this suggests a mere conduit or liaison function. It makes a representative the local embodiment of a foreign controller, an entity within the jurisdiction on which the GDPR can bite with legal force. Further, the purpose of Art.27.5 is to put beyond doubt that which is only in any doubt in the first place under the Claimant's interpretation – that the representative does have legal liability, but that it is in addition to, not in substitution for, the controller's.

Proposed Aids to Interpretation**(i) The Scheme of the GDPR's Operative Provisions**

17. The broad scheme of the GDPR is to protect personal data privacy by imposing obligations on controllers (who determine the purposes and means of data processing), and processors (who process on behalf of controllers). Those obligations are enforceable in two distinct ways: by data subjects asserting corresponding legal rights in court, and through the regulatory powers of the ICO. Regulatory enforcement and data subject enforcement are complementary, and overlapping.
18. The GDPR makes extensive reference, accordingly, to the obligations of controllers. Among these are the liabilities the Claimant seeks to enforce in the underlying claim

Approved Judgment

in this case, through his reciprocal legal rights to erasure and rectification of data, and to compensation. These include restrictions on processing, and obligations to notify rectification and erasure to third parties. The parties' rival interpretations of Art.27 naturally lead them to make rival points about whether such references to controllers in the GDPR are to be read as inclusive, or alternatively exclusive, of references to representatives. In itself that is, of course, largely to restate the question.

19. The GDPR is divided into chapters. After the general provisions of Chapter I, Chapter II sets out the data protection principles, Chapter III the rights of data subjects and Chapter IV the obligations of controllers and processors. Articles 24-31 comprise the first Section (headed '*general obligations*') of Chapter IV. Articles 24 and 25 deal with the broad responsibilities of controllers. Article 26 makes specific provision for joint controllers (including requiring transparency about their respective roles and providing for enforcement against each joint controller). The Defendant points to the absence of equivalent explicit provision for joint and several liability between controllers and representatives in Art. 27; the Claimant says that is because the position is simpler – the representative steps into the controller's shoes.
20. Art.27 is sandwiched between these provisions and the remainder of the first section of Chapter IV, which deals with the duties of processors and a small number of shared or joint responsibilities. The logic of its position reflects the distinctive status of Art.3.2 controllers: not established, but subject to GDPR compliance. The duty to appoint a representative is their distinguishing obligation. The rest of Chapter IV deals with data security and other general obligations. Among them is the requirement for controllers to appoint a 'data protection officer' (Art.39.1(e)) with a list of distinct duties including *to act as the contact point for the supervisory authority on issues relating to processing*. This might be contrasted with the language of Art.27.
21. Chapter VIII of the GDPR deals with remedies, liability and penalties. The Defendant draws attention to the careful provision made in Art.82 about the right to compensation *from the controller or processor* for any damage suffered by infringement of the GDPR. This includes provision in Art.82.2 limiting the liability of processors to cases where they have failed to comply with obligations in the GDPR *specifically directed to processors* or where they have acted outside the instructions of their controller. It also includes the provision in Art.82.4 for cases of multiple responsibility for the damage: *each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject*. Provision is made for claim-back indemnities in Art.82.5. Again, the Defendant points to the absence of equivalent provision for representatives and queries why a (mere) representative would be more exposed than a processor. The Claimant reiterates the simplicity of his position – a representative is treated with exact equivalence to its controller – and notes the express link in Art.82.4 between joint and several liability and the GDPR policy of ensuring *effective* compensation of the data subject.
22. There are a limited number of points at which the GDPR addresses the position of representatives separately and distinctly from that of controllers.

Approved Judgment

- i) Arts.13 and 14 require the controller to provide the identity and contact details of its representative, as well as its own, to a data subject when it obtains their data.
- ii) Art.30 imposes duties on a representative, in addition to those of a controller, to maintain detailed records of processing activities.
- iii) Art.31 imposes duties on controllers *and* representatives to co-operate, on request, with the ICO in the performance of its tasks.
- iv) Art.58 requires the ICO's *investigative* powers to include the ability to order not just a controller but also a representative to provide any information the ICO requires for the performance of its tasks; the ICO's *corrective* powers by contrast are not (separately) applied to representatives.

(ii) The GDPR Recitals

- 23. The parties agree as to the correct general approach to recitals in an instrument such as the GDPR. Recitals explain and give policy reasons for the operative provisions. They may be used as an aid to construction of operative provisions, or to fill in more detail. But they are not intended to have normative, or distinct legal, effect. If and to the extent that recitals and operative provisions appear to be in conflict, then precedence must be given to the operative provisions.
- 24. The GDPR is noteworthy for the extent and detail of its 173 recitals. They provide an extensive commentary on the operative text of the GDPR. Recital 80 provides the relevant commentary on Art.27. It says this:

Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body.

The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority.

The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation.

Approved Judgment

The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation.

Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation.

The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

25. The Claimant places considerable reliance on Rec.80 as an aid to the construction of Art.27, especially the last sentence of Rec.80. He draws attention to the repeated provision that a representative is to *act on behalf of* the controller – including *with regard to [the controller’s] obligations* under the GDPR. The requirement to *act on behalf of* clearly goes considerably further, he says, than envisaging a mere conduit role. He says that the final sentence is clear and explicit as to the (non-substitutive) liability of a representative: it will itself be liable to enforcement in respect of a controller’s breach of its obligations.
26. The Claimant says that considerable, and if necessary determinative, weight should be given to Rec.80. He draws a parallel with *Blanche v EasyJet* [2019] EWCA Civ 69, where the Court of Appeal applied a recital, which it considered to be clearly expressed and in accordance with the policy underlying a Regulation, to determinative effect in resolving the scope of a duty imposed by that Regulation.
27. The Defendant finds no such effect in Rec.80. It says that, at its highest, the final sentence is limited to (regulatory) *enforcement proceedings* as opposed to (data subject) judicial proceedings such as the underlying claim in the present case. It says that, beyond that, to the extent that it is argued to support the Claimant’s position, it is either inconsistent with Art.27 and the wider scheme of the GDPR, or is impermissibly attempting normativity. In either case it should be disregarded or given little interpretative weight. The Defendant distinguishes *Blanche v EasyJet* as concerned with the interpretation of a specific phrase in the operative part of the Regulation (*‘extraordinary circumstances’*). Here, it says, an attempt is being made to use a recital not just to fill out the meaning of an operative term but to found an entire structure of liability which is simply absent from the operative terms of the GDPR.

(iii) EDPB Guidelines 3/2018

28. Section 3 of Chapter VII of the GDPR creates a European Data Protection Board (EDPB), bringing together heads of national regulators. The Information Commissioner was a member. Art.70 tasks the EDPB with ensuring consistent application of the GDPR, including by issuing guidelines.

Approved Judgment

29. The EDPB prepared draft guidelines on the territorial scope of the GDPR (Art.3), and issued them for public consultation in November 2018. They were amended and adopted as Guidelines 3/2018 in November 2019. The Guidelines address the Art.3.2 situation and aim to provide clarification about the appointment, responsibilities and obligations of Art.27 representatives.
30. Under the heading '*Obligations and responsibilities of the representative*', the Guidelines emphasise the importance of providing the representative's identity and contact details to data subjects under Arts.13 and 14. They state: '*While not itself responsible for complying with data subject rights, the representative must facilitate the communication between data subjects and the controller or processor represented, in order to make the exercise of data subjects' rights effective.*'
31. They also deal with the record-keeping requirements under Art.30, imposed on both controller and representative. They say it is the controller who is responsible for the content and updating of the record, and must simultaneously provide the representative with all accurate and updated information so that the record can also be kept and made available by the representative. It is, however, the representative's distinct responsibility to *provide* the record in accordance with Art.27, for example when being addressed by the ICO under Art.27.4.
32. The Guidelines continue:

As clarified by recital 80, the representative should also perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. In practice, this means that a supervisory authority would contact the representative in connection with any matter relating to the compliance obligations of a controller or processor established outside the Union, and the representative shall be able to facilitate any informational or procedural exchange between a requesting supervisory authority and a controller or processor established outside the Union.

With the help of a team if necessary, the representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication should in principle take place in the language or languages used by the supervisory authorities and the data subjects concerned or, should this result in a disproportionate effort, that other means and techniques shall be used by the representative in order to ensure the effectiveness of communication. The availability of a representative is therefore essential in order to ensure that data subjects and supervisory authorities will be able to establish contact easily with the non-EU controller or processor. In line with Recital 80 and Article 27(5), the designation of a representative in the Union does not affect the responsibility and liability of the controller or of the

Approved Judgment

processor under the GDPR and shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves. The GDPR does not establish a substitutive liability of the representative in place of the controller or processor it represents in the Union.

It should however be noted that the concept of the representative was introduced precisely with the aim of facilitating the liaison with and ensuring effective enforcement of the GDPR against controllers or processors that fall under Article 3(2) of the GDPR. To this end, it was the intention to enable supervisory authorities to initiate enforcement proceedings through the representative designated by the controllers or processors not established in the Union. This includes the possibility for supervisory authorities to address corrective measures or administrative fines and penalties imposed on the controller or processor not established in the Union to the representative, in accordance with articles 58(2) and 83 of the GDPR. The possibility to hold a representative directly liable is however limited to its direct obligations referred to in articles 30 and article 58(1) a of the GDPR.

33. This last paragraph had undergone a degree of revision in response to the consultation exercise. The draft put out for consultation had said this:

It should however be noted that the concept of the representative was introduced precisely with the aim of ensuring enforcement of the GDPR against controllers or processors that fall under Article 3(2) of the GDPR. To this end, it was the intention to enable enforcers to initiate enforcement action against a representative in the same way as against controllers or processors. This includes the possibility to impose administrative fines and penalties and to hold representatives liable.

34. The Defendant says the difference between the two versions shows a clear rejection by the EDPB of the interpretation proposed by the Claimant, whatever its first thoughts might have been. It says the final version of the Guidelines is clear as to the important, but limited, role of the representative in providing contact and liaison functions between foreign controllers on the one hand, and local enforcement authorities and data subjects on the other. It may be inferred that these functions extend up to and including accepting service of enforcement process. But a representative has neither 'direct' nor 'substitutive' liability for the obligations of controllers.
35. The Claimant makes a number of points. First, the earlier draft of the Guidelines shows the EDPB at the very least considered his preferred interpretation consistent with the scheme and policy of the GDPR. Second, he is contending for neither 'direct' nor 'substitutive' liability. He accepts the need to qualify liability with 'direct' in referring to the distinct obligations imposed on representatives (record-keeping, etc). He accepts the liability of a representative is not substitutive for

Approved Judgment

(exclusive of) a controller's liability. He contends for 'representative' liability, the representative standing in the shoes of the controller. He considers that consistent with the Guidelines. The Guidelines are in any event just that: non-binding and evidently mutable.

(iv) The Position of the ICO

36. The ICO has not issued specific guidance on the role and function of representatives. It issued general guidance on '*Data Protection at the end of the transition period*' in September 2019. This had two short sections on the *appointment* of representatives: the first dealing with the situation of UK controllers needing to appoint a representative in the EEA after Brexit, and the second dealing with foreign controllers needing to appoint a representative in the UK. It made reference to and brief comment on the EDPB Guidelines on territorial scope, but of course this was before the final version was adopted in November 2019.

37. The Defendant wrote to the ICO on 9th March 2021, enclosing documents in these proceedings and inviting the Information Commissioner to express a view on the interpretative question at issue. A response from the ICO on 30th March offered these thoughts:

It is the view of the ICO that the role of an Article 27 representative of overseas data controllers and processors is limited to that of conduit of communications between the overseas entity and the ICO or relevant data subjects.

Therefore the ICO is not seeking an interpretation of Article 27 that allows representatives to be held directly liable should a controller or processor they represent fail in their data protection obligations.

...

An Article 27 representative does not undertake any other business activity related to the processing of the controller or processor, other than acting as a contact point for data subjects and the ICO. From the point of view of the ICO, the existence of a representative makes it easier to take action against a controller by acting as a conduit, but any enforcement action is directed against the controller itself.

38. The ICO's reply referenced the provisions of the EDPB Guidelines set out above and emphasised the points noted about the absence of 'substitutive liability' and the limitations of 'direct liability'.

39. Some further correspondence between the parties and the ICO ensued. The Claimant queried the ICO's response and its consistency with Rec.80. A reply of 19th April 2021 stated that the 30th March response had taken account of Rec.80, but considered Art.27.4 the definitive provision on the role of Representatives and that it 'prevails'.

Approved Judgment

The reply again considered that view supported by the EDPB Guidelines. In this correspondence the ICO emphasises the role of the Information Commissioner as a member of the EDPB at the time the Guidelines were being prepared, a role in which it describes the ICO as having been heavily involved.

40. The ICO has not, however, sought to intervene in the current proceedings or otherwise taken a formal position on or role in them.

(v) The Data Protection Act 2018

41. The Data Protection Act makes limited further provision about representatives, supplementary to the GDPR. It adopts in s.181 ‘representative’ as a defined term from Art.4(17). Sections 142 and 143 make provision for the issue of ICO ‘information notices’ to representatives as well as controllers and processors, further to the ‘investigative powers’ provisions of Art.58.1. Just as the Art.58.2 ‘corrective powers’ provisions make no mention of representatives, the Act is similarly silent in the provision made at section 149 for the ICO to issue ‘enforcement notices’ to controllers and processors (and at section 167 for a court to issue ‘compliance orders’ to controllers and processors).

(vi) Article 79 GDPR, the EU Charter and the Principle of Effectiveness

42. Article 79 is headed ‘*Right to an effective judicial remedy against a controller or processor*’. Art.79.1 provides as follows:

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

The Claimant points out this reflects the general provision made in Art.47 of the EU Charter that everyone whose rights have been guaranteed by the law of the Union has the *right to an effective remedy* before an independent tribunal if those rights are violated.

43. The parties agree that the principle of effectiveness is available as an aid to interpretation in the present case. It requires that the right to an effective judicial remedy must be practical and effective, and not theoretical and illusory. The enforceability of rights must be considered in real world terms. The exercise and enforcement of rights must not be rendered practically impossible or excessively difficult.
44. The Claimant prays the principle of effectiveness in aid on the basis that Art.3.2 controllers are clearly subject to GDPR obligations, and that the provisions of Art.27 are directed to the effectiveness of the enforcement of those obligations. He says the Defendant’s interpretation of Art.27 would render it excessively difficult for data subjects to enforce their rights against foreign data controllers. It would be arbitrary, and undercut the aim of consistent and effective protection for data subjects.

Approved Judgment

45. The Defendant says the principle of effectiveness applies, but does not produce the result sought by the Claimant. Data subjects clearly do have rights and remedies in respect of foreign data controllers; they are enforceable against them in the normal way any rights are enforced extra-jurisdictionally.

(vii) ‘Representatives’ in other Regulations

46. The obligation on foreign data controllers to appoint a local representative is a relatively recent addition to the data protection regime. But representatives appear in other EU instruments. The Defendant cites some examples.
47. One is EU Regulation 2017/746 which deals with certain diagnostic medical devices. Art.11 of that Regulation provides that where the manufacturer of a device is not established in a Member State, the device may be placed on the market only if the manufacturer designates *a sole authorised representative*. Detailed provision is made about what that designation or mandate is to require the representative to do, including regulatory verification of the manufacturer’s compliance. It provides that *‘the authorised representative shall be legally liable for defective devices on the same basis as, and jointly and severally with, the manufacturer’*.
48. Regulation 2017/746, like the GDPR, makes a defined term of ‘authorised representative’. By Art.2(25) it means *‘any natural or legal person established within the Union who has received and accepted a written mandate from a manufacturer, located outside the Union, to act on the manufacturer’s behalf in relation to specified tasks with regard to the latter’s obligations under this Regulation’*.
49. It also includes a relevant Recital. Rec.34 says this:

For manufacturers who are not established in the Union, the authorised representative plays a pivotal role in ensuring the compliance of the devices produced by those manufacturers and in serving as their contact person established in the Union. Given that pivotal role, for the purposes of enforcement it is appropriate to make the authorised representative legally liable for defective devices in the event that a manufacturer established outside the Union has not complied with its general obligations. The liability of the authorised representative provided for in this Regulation is without prejudice to the provisions of Directive 85/374/EEC, and accordingly the authorised representative should be jointly and severally liable with the importer and the manufacturer. The tasks of an authorised representative should be defined in a written mandate. Considering the role of authorised representatives, the minimum requirements they should meet should be clearly defined, including the requirement of having available a person who fulfils minimum conditions of qualification which should be similar to those for a manufacturer's person responsible for regulatory compliance.

50. The Defendant draws attention to the differences between these provisions about representatives of foreign manufacturers, where express provision for a *‘pivotal role’*,

Approved Judgment

detailed mandate, relevant qualifications and legal liability is made, and the provisions of the GDPR. The Claimant draws attention to the similarities, including by reference to the centrality of ‘*acting on behalf*’ and ‘*in relation to obligations*’ under the instrument, and also to the policy equivalences of ensuring compliance by foreign operators by imposing an obligation to appoint a local representative. He says that the GDPR does the same thing, albeit by contrasting means.

Analysis**(i) General Approach**

51. I approach Art.27 bearing all of these aids to interpretation in mind. No others are proposed; it is not, for example, suggested that the negotiation history of the relevant parts of the GDPR, or the practice of other Member States, is of assistance. The question of the combined effects of Art.27 and Rec.80 is nevertheless not a new one; it has been noted by academics and legal commentators before now. I was alerted to the observations of Rosemary Jay in her authoritative textbook *Data Protection Law and Practice*. She notes the point to be ‘not without difficulty’ and alludes to the inevitability of ‘engrossing academic debate’. It is not, however, suggested by the parties that further assistance is to be obtained from perusal of the literature.
52. The point itself is not an ‘academic’ or theoretical one. It was said before me to bear acutely on the exposure of representatives to liability, and of data subjects as to the effectiveness of their rights. The idea that resolving any point of law can be a ‘pure’ or abstract exercise in parsing language is anyway a dangerous proposition, and certainly so when looking at one part of a mature and systematised legal structure with a highly practical purpose. In the global information age, data protection – the law and practice of personal information privacy – is above all an intensely practical regime.
53. There are other dangers in the present exercise. It would be a mistake, for example, to consider the functions of an Art.27 representative in isolation, when on any basis it is a relational role. Data protection itself is a regime based on the triangular relationship between data subjects with rights, data controllers with duties, and the ICO with regulatory functions (Data Protection Act 2018 section 2). Representatives occupy a place in that triangular relationship, and understanding it requires a suitably triangulated perspective.
54. There is also a danger in starting with the aspect raised by this application – enforcement and litigation – rather than with a sound grasp of what we can *know* from the GDPR about appointing a representative and what it must do. While data protection is given force by compulsive powers and remedies, it works day to day on the basis of established and shared practical protocols to enable the vast and vital data flows which power modern life consistently with fair protection for individuals. Enforcement is key, but exceptional, relative to the sheer everyday ubiquity and systematised realities of data processing. That is why the regulatory role is such an important part of data protection; getting systems right first time is the overwhelming priority for all involved.
55. It is important also not to lose sight of the fact that the policy given fine-tuned effect in data protection law involves a *balance* – between facilitating the free flow of data

Approved Judgment

on which modern life relies and protecting individual rights which have their ultimate origin in Art.8 ECHR. Data processing is global business, and data protection law is both a market regulation measure with a specific transnational application regime, and a species of detailed privacy protection. The opening recitals of the GDPR make important contextual reading.

56. I approach the question, therefore, by standing back to look at the uncontroversial, everyday role of a representative, and its place in the triangle of relationships between controllers, data subjects and the ICO. From that vantage point, I return, via the language of Art.27 and the aids to construction offered, to the question of whether or not the Claimant has a legal basis for suing the Defendant in this case.

(ii) The Controller's Perspective

57. The starting point in understanding the role of representatives is the territorial scope provision of Art.3.2. That applies domestic data protection law to certain processing activities of foreign controllers. So beneath the question about the role of representatives is the issue of what it means to say that data protection law applies, where data subjects are within the jurisdiction but the controller is not. The Claimant says that representatives provide the whole answer, representing foreign controllers for enforcement purposes. But the issue itself – how data protection sounds extra-jurisdictionally – is multi-faceted; the GDPR comes at it from more than one angle.
58. The territorial scope provisions are not the only aspects of the GDPR of particular potential relevance to foreign controllers. They sit alongside the third country data transfer regime of Chapter V. This is a powerful and sophisticated mechanism for the protection of data subjects and the incentivisation of compliance by third countries and extra-jurisdictional data controllers. In essence (again, the relevant recitals give policy context), it provides for the free flow of personal data between GDPR countries and foreign countries if the European Commission has formally decided that those countries' legal systems provide 'adequate' data protection, including as to enforcement (Art.45). Otherwise, transfer of personal data to foreign countries is permitted only subject to specific *enforceable* safeguards (Art.46), of which standard forms have been developed.
59. Data export, and the processing to which Art.3.2 applies, are different activities. But although the one does not necessarily imply the other, Art.3.2 controllers may have to think about Chapter V export conditionality too. Taken together, these provisions aim at consistently high levels of extra-jurisdictional protection for data subjects, and consistently free data flows for the mutual benefit of citizens and reputable, *compliant* or regulated, foreign controllers and consumers of data processing. In practice, of course, the picture varies considerably. Other countries' legal systems can and do strike different balances between the free flow of data and protecting individual data privacy. Full 'adequacy' status has so far been granted to relatively few third countries. The burdens of the applicable local legal and regulatory regime on the one hand, and the benefits of access to the data and data subjects of GDPR-regulated nations on the other, are business considerations which weigh importantly on controllers in deciding where to locate and how to operate their businesses. And it is not just an individual business matter for them; it is of potential national strategic importance for countries seeking to maximise access to GDPR-regulated activities more generally.

Approved Judgment

60. The appointment by an Art.3.2 controller of a representative is, in and of itself, an important signal that the controller is engaging with the GDPR, understands its scope provisions, and accepts the conditionalities it imposes on its access to data and data subjects. It signals, in other words, a recognition of the bargain involved: the burden to be shouldered for the benefit to be gained. It is an acceptance of the application of Art.3.2 and a signal of good intent. As Miss Skinner QC, Leading Counsel for the Defendant in this case, put it, the bad guys do not appoint Art.27 representatives.
61. Art.27 makes clear that, at the very least, a representative is a mandated, permanent, established, intra-jurisdictional presence representing an extra-jurisdictional controller. The controller cannot rely on access to Art.3.2 data subject markets or monitoring without it. It is also a generalised presence. A representative can expect to be addressed *on all issues related to processing* by the foreign controller. And it is a presence which makes a contribution to the reliability of the controller's GDPR *compliance* in circumstances in which there is a degree of practical *risk* to the position of data subjects.
62. That is underscored by the Art.13/Art.14 requirement to include a representative's identity and contact details in the package of information a controller must provide to data subjects when it acquires their data. Giving information at the point of data acquisition is a cornerstone of the duties applying to all controllers. It is a fundamental transparency requirement, to give data subjects not only a clear view of what is being done with their data and why, but also a snapshot of the legal basis relied on and an overview of their rights. The package of mandatory information includes the identity and contact details of the controller itself, full details of any intended third-country data transfer, the 'adequacy' status of that country (which may include the country in which the controller is established), and any 'safeguards' relied on. So the package gives data subjects the fullest possible overview of a controller's claim to GDPR compliance.
63. A similar point arises with the Art.30 record-keeping obligations imposed expressly on representatives. This is not an exercise in back-office bureaucracy. The records which must be kept are a full account of the point-by-point particulars of the controller's operation (including as to third-country transfers) on which its compliance with the GDPR depends and may be judged. They are disclosable on demand to the ICO, precisely as such. Importantly, they map across to the information which must be disclosed to data subjects when they exercise their cornerstone right of subject access (Art.15) as further discussed below. A representative is accordingly under clear legal obligations, as the mandatory presence of the controller within the jurisdiction, to ensure by this means that a foreign controller is kept primed for full local transparency as to its compliance status.
64. The GDPR therefore makes the representative the subject of mandatory appointment and, once appointed, of specified legal obligations. The controller must 'mandate' the representative as such. That indicates a measure of formality, and the controller's acceptance that, for its own part, it will enable the representative to fulfil the obligations that go with the appointment, not least by furnishing it with the information forming the content of its record-keeping functions. A contractual relationship suggests itself (the ICO envisages a 'simple service contract') but is not expressly specified.

Approved Judgment**(iii) The Regulator's Perspective**

65. The importance of the provision in Art.30.4 for representatives to make any and all aspects of the full Art.30 record available to the ICO on request is hard to overstate. After the primary source material of the data and processing operations themselves, the Art.30 record is the best and most complete secondary source of compliance information available within the jurisdiction. It is the obvious starting point for the exercise by the ICO of its functions in relation to the foreign controller.
66. It is also fully backed by the reciprocal investigative powers of the ICO under Art.58.1(a). The legal power for the ICO to order a representative to *provide any information it requires for the performance of its tasks* leaves no room for doubt about the importance of the representative's function as local custodian of the full record of the controller's operation, and therefore its role in guaranteeing the regulatory transparency of that operation.
67. This is also to be understood from the general obligation imposed by Art.31 – cumulatively on controller and representative – to co-operate with the ICO in the performance of its tasks. That sets a tone in encouraging a supportive rather than defensive stance towards the regulator. It also reinforces the transparency theme in the data protection regime.
68. Making it an express and specific responsibility of local representatives is significant. The task of the ICO is indisputably more complex and difficult where foreign controllers are concerned. There may be additional practical difficulties – of language, time zone, business culture or national politics, for example – to overcome. There may be additional legal complexities – as to 'adequacy' status or particular 'safeguards' for data transfer, or international law considerations – to be navigated. The duty to co-operate is recognisable as an active, genuinely ambassadorial, role for a representative: being ready to explain such matters to the ICO, and being equally ready fully to understand and acknowledge any ICO request for co-operation, and to work together with a controller to comply with it.

(iv) The Data Subject's Perspective

69. Two very broad propositions might be risked in an attempt to distil the perspective of data subjects to a few general principles. The first is that data subjects are basically entitled to two things: to have their data processed in accordance with the duties imposed on controllers (compliance), and to know who is doing what with their data in the first place (transparency). The second broad proposition is that, although there is no formal hierarchy of enforcement, the powers and duties of the ICO are there to secure entrenched and systemic compliance, and to tackle non-compliance with a full toolkit of regulatory responses, rather than routinely leave data subjects with the considerable burden of enforcing their rights through litigation.
70. The right of 'subject access' might be considered the primary and fundamental data subject right. It has two functions. The first is that, together with the right to the provision of information at the point of data acquisition by the controller, it is the principal transparency right – the 'right to know' whether any controller has your personal data and if so what it is doing with it. That is an end in itself. The second function is instrumental. Subject access can provide a first step in monitoring or

Approved Judgment

securing compliance. The knowledge it provides may allay any concerns, or furnish a basis for further investigation – for example if the data subject is not satisfied that data are accurate or being processed compliantly. It may equip a data subject to seek help and advice from the ICO. It may provide a basis for the exercise of investigatory powers by the ICO. It may be the start of a process which ultimately leads to enforcement by the ICO or by data subjects themselves.

71. Art.27.4 is clear that representatives may be addressed in particular by data subjects on all issues related to processing. Since the right of subject access is a primary data subject right, there is no reason to doubt its inclusion in this formulation. The right comprises being given access to the personal data themselves and the right to specified ancillary information about the processing (Article 15). Much of the ancillary information is information within the ambit of the record-keeping duties of representatives. Data subjects are also entitled to be informed of their right to lodge complaints with the ICO. Representatives are well equipped to assist data subjects in the exercise of their rights of subject access, and are bound to assist the ICO in the performance of *its* tasks in upholding those rights in practice.
72. Where the knowledge given by subject access leads to compliance concerns by a data subject, then the spotlight moves from the record-keeping functions of representatives to their obligations to co-operate with the ICO and their subjection to the ICO's investigatory powers. From the data subject's point of view, the representative provides a local and accessible point of engagement with a foreign controller (a relationship in which there may be a substantial imbalance of power), understanding and facilitating the exercise of subject access rights, and staying engaged if the data subject has concerns, up to and including the involvement of the ICO and the potential service of process.

(v) Overview of the Role and Function of Representatives

73. I do not consider any of the above analysis to be controversial. It sets out what we can *know* about representatives from the GDPR, and the context of the question raised by this application. Having considered the day-to-day role of the representative from all three relevant perspectives, it remains to superimpose them and reflect on the three-dimensional picture that provides.
74. At the least, the picture which emerges is of a considerably fuller role than a mere postbox '*to be addressed*'. Even the language of 'conduit' or 'liaison' does not fully capture the job the GDPR gives to representatives. The role is an enriched one, active rather than passive. At its core is a bespoke suite of directly-imposed functions. These are crafted to fit together with, and belong in the triangle of, the relationships between controller, ICO and data subject. The job focuses on providing local transparency and availability to data subjects, and local regulatory co-operation. And the appointment is of course an opportunity for foreign controllers to give representatives any other ambassadorial - 'shop window' or customer-facing - functions, additional to the core 'mandate' functions, as they consider desirable demonstrations of their compliance credentials.
75. All of this is because the processing is not being undertaken in the context of an establishment of a controller/processor within the jurisdiction. The Art.27 system is set up, says the Defendant, precisely because the distinguishing feature of non-

Approved Judgment

established controllers is that they are not directly subject to the jurisdiction of the ICO and the courts as a matter of the scope of national law. It is a special system *in the alternative*. The Claimant says, on the contrary, that it is precisely because there is no other way to enforce against non-established controllers that the legal liability of representatives must be seen as the final piece of the jigsaw.

76. For the reasons which follow, ‘representative liability’ is in my view harder than the alternative to reconcile with the scheme of the GDPR and the interpretative aids set out above. But Rec.80 challenges that view and demands pause for thought before any conclusion is reached.

(vi) ‘Representative Liability’ and the Scheme of the GDPR

77. First, the GDPR creates the representative role with care and specificity, and does not *unambiguously* provide for the liability for which the Claimant contends. That is not (just) the linguistic point that if the GDPR had intended that result it would and should have said so more clearly. It is a point about the consistency and logic of the GDPR’s overall scheme for the global dimension of data processing.
78. The extra-jurisdictional reach of the GDPR does not lack ambition. Art.3.1 provides for unlimited, global, scope for the activities of controllers established within the jurisdiction, wherever in the world they take place. Chapter V *prohibits* transfer of data out of the jurisdiction, including to foreign controllers, unless certain conditions are fulfilled: effectively requiring third countries or their controllers to comply in whole or in part with the GDPR’s protections if these data flows are to happen at all. These policies are stated explicitly and articulated coherently and in detail in the scheme of the GDPR. The policy for which the Claimant contends effectively requires relevant foreign controllers to adopt a form of establishment within the jurisdiction, fully on-shoring their liability and putting them on a par with established controllers, as a precondition of compliant processing of the data in question. That is an ambition which is not asserted in anything like equivalent terms in the GDPR.
79. It is stated, and realised, to a limited degree in other instruments. The contrast is interesting, again not to make a drafting point but to illustrate policy difference. Making a local representative personally liable in relation to ‘*specified tasks*’ of overseas manufacturers of medical devices is one thing: a policy of complete control over the quality of particular goods entering the market. Making a local representative personally liable in relation to the full suite of data controller responsibilities is an incomparably more ambitious policy which it is hard to reconcile with much more shy articulation.
80. That leads directly into a second problem for ‘representative liability’: practicality. Standing in the controller’s shoes for enforcement purposes implies representatives’ ability to provide, or require the controller to provide, remedies which involve direct access to and operations on the personal data themselves. That includes rectification and erasure of data, and giving subject access not just to ancillary information but to the actual data. That is nowhere discernibly provided for in the GDPR (or the 2018 Act).
81. The GDPR neither expressly confers those functions on representatives nor places them under anything like the duties controllers and processors – and data protection

Approved Judgment

officers – are under, concomitant to their access to personal data. The Claimant says that all necessary powers and indemnities would be supplied via the ‘mandate’ – the contract between controller and representative. The GDPR does not itself expressly obligate a contract of that crucial nature. It would be a contract to which both the ICO and data subjects were strangers; and since there are no publication or access provisions relating to the mandate it would be entirely untransparent to them.

82. It is not apparent that the GDPR envisages representatives processing personal data themselves at all, whether directly or via contractual powers to compel controllers. ‘Standing in the shoes’ of controllers for enforcement and remedial purposes sounds like a simple proposition. It is not. The enforcement powers of the courts and the ICO mirror the full range of the duties of controllers and processors which are imposed because of the power *they have on a day to day basis* over how and why data are processed. A representative does not have that; it is not constituted as a controller or processor in its own right.
83. If the policy of the GDPR had been to require foreign controllers to appoint and establish local *processors*, within the terms of Art.28, to access the data on the controller’s behalf for the purposes of substantiating local liability, it could have done that. But representatives are different from processors. The representative’s ‘mandate’ bears no visible resemblance to the processor’s contract, as extensively provided for by Art.28.3-9. The core job the GDPR specifically gives representatives *has to do with* (is ‘*related to*’) the activities of a controller or processor – processing personal data – but stops short of *doing* those activities and becoming one. How would it then deliver remedies requiring operating on (processing) personal data?
84. That leads to a third problem for ‘representative liability’. If a representative stands in the shoes of a controller, the package of duties the GDPR imposes directly on it is otiose. No visible difference need be made between the investigative and corrective powers of the ICO such as Art.58 provides for, if both can be exercised against a representative. A representative need not be given special record-keeping responsibilities if it is liable to guarantee full transparency (information provision and subject access) rights in any event.
85. A fourth problem is that what the GDPR *does* say about the liability of representatives appears directed at excluding rather than emphasising it. The Claimant argues for the compatibility of ‘representative liability’ with this exclusive language on the basis that it is *additional* to both ‘direct’ liability for representatives’ specified functions and the ‘substitutive’ (replacement) liability which is excluded. But if it is a species of joint and several liability, it is not clear from the GDPR how it works. That is not just a matter of the practicalities of enforcement, but of substantive transparency (cf Art.26). And since ‘representative liability’ surely cannot be cumulative with controller liability, it must ‘affect’ (and ultimately discharge) it. That is hard to reconcile with what Art.27.5 says. It is also hard to understand why an enforcer would ever do anything else, always assuming the representative were fully ‘mandated’. Perhaps after all ‘representative’ and ‘substitutive’ (contracted-out) liability is conceptual distinction without practical difference.
86. The alternative view – that the GDPR gives representatives a bespoke, limited but important role which supports and is ancillary but not alternative to extra-jurisdictional enforcement against Art.3.2 controllers – raises none of these internal

Approved Judgment

difficulties. It is a role to be understood as predicated on a basic willingness of foreign controllers to accept the expectations of compliance with Art.3.2. It recognises that the GDPR does have *some* jurisdictional limitations, notwithstanding the ambitions of its reach, and ultimately extra-jurisdictional enforcement is a matter of international law. On that basis, the representative function is clearly recognisable as a useful and beneficial addition to the general scheme of the GDPR.

(vii) ‘Representative Liability’, the EDPB Guidelines and Other Context

87. Among other things, the GDPR is a market harmonisation measure and the primary function of the EDPB is to enhance *consistent* interpretation of the regime. On the one hand that does acknowledge that there is legal space for variation in interpretation in the first place, but on the other it is intended to occupy some of that space. The Guidelines therefore have weight which goes beyond expert commentary on the primary text. They do not constitute law but they are an important indicator of whether or not ambiguity genuinely exists in the text and, if it does, the best approach to understanding it. They have to be given commensurate weight.
88. The Guidelines leave little or no space for ‘representative liability’. They make clear that a representative *‘is not itself responsible for complying with data subject rights’*. They make clear that it is the controller which remains responsible for the content of the record which both controller and representative must maintain; the controller must put the representative in a proper position to fulfil the latter’s discrete responsibility (not the other way around). Co-operating with the ICO means in practice that the representative is available to be contacted and will *‘facilitate any informational or procedural exchange’* between the ICO and the extra-jurisdictional controller, up to and including addressing enforcement process imposed on the controller *‘through’* the representative. They expand, in other words, over several paragraphs, on what is set out above as being the bespoke role given to a representative by the GDPR. They stop short there.
89. Where the Guidelines address the legal liability of representatives at all, they do so in exclusionary terms: *‘The GDPR does not establish a substitutive liability of the representative in place of the controller or processor it represents in the Union’* and *‘The possibility to hold a representative directly liable is however limited to its direct obligations referred to in articles 30 and 58.1 of the GDPR’*. These provisions may not be absolutely inconsistent with the GDPR having placed a representative in the shoes of a controller across the entirety of its legal and regulatory obligations. But the resounding silence of the Guidelines where one would expect to see some expansion of, or at the very least unambiguous reference to, that liability, is striking.
90. It is all the more striking when the text of the Guidelines is compared to the rejected text of the consultation draft. It is not simply that the Guidelines *deliberately* do not say that there is a possibility to hold representatives liable. It is the important new provision made in its place. Immediately after the passage set out at paragraph 32 above, and in conclusion, the Guidelines add:

The EDPB furthermore highlights that article 50 of the GDPR notably aims at facilitating the enforcement of legislation in relation to third countries and international organisations, and

Approved Judgment

that the development of further international cooperation mechanisms in this regard is currently being considered.

91. Article 50 is the concluding provision of Chapter V of the GDPR. It is headed ‘*International cooperation for the protection of personal data*’. It provides as follows:

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

92. This is a provision which acknowledges the limitations of the legal reach of the GDPR and addresses the territory which lies beyond, where international co-operation and international law, including mutual enforcement agreements, are the only effective means of securing data protection. A duty to advance those means is placed on the Commission and the national regulators – the membership of the EDPB. The relevance of making this reference in the Guidelines, in explaining the role of representatives, can only be to acknowledge that they do *not* provide a solution to enforcement in Art.3.2 cases and that ultimately the realities of extra-jurisdictional enforcement must be addressed instead. The representative is an important part of addressing those realities in furtherance of securing compliance, and of promoting co-operation. But it does not supersede or obviate them.

93. That is also where the argument from general principles about the right to effective remedies, judicial or otherwise, ends up. I was shown no authority to suggest that this principle includes full *extra-territorial* effectiveness and dissolving the limits of jurisdiction, either in general, in relation to the GDPR, or in relation to non-established controllers in particular. Effectiveness is not a globally unlimited and absolute proposition. Data subjects have effective remedies against Art.3.2 controllers insofar as international law can provide for them. *In addition* and ancillary to that, the GDPR ensures that Art.3.2 controllers, wishing to engage with the regime and demonstrate compliant intent, appoint representatives as visible day-to-day

Approved Judgment

participants and embassies of local co-operation and support. The principle does not itself entitle data subjects to *more* effective remedies. Any such entitlement has to be found elsewhere. The argument from the obligation to provide an effective remedy, to the plenipotentiary liability of representatives, appears largely to assume what it needs to prove, namely that the GDPR itself provides or requires more.

94. I give weight to the perspective of the ICO - not so much as an aid to the interpretation of the GDPR as a legal text (notwithstanding the undoubted expertise of our national regulatory authority on the proper interpretation of data protection law), as because of what it says about its practical approach to the exercise of its own functions in relation to representatives. The regulator/representative relationship is the issue which can most clearly be seen to have undergone amendment in the process of finalising the EDPB Guidelines. As well as being under legal obligations to ensure consistency, EDPB members are especially well placed to do so in the practice of their own functions. It is also a matter on which GDPR expectations of consistency of approach and practice might be thought important. The ICO has no expectation of holding representatives liable or available for enforcement purposes other than as clearly provided: in relation to their own bespoke functions and in providing co-operative assistance.

(viii) ‘Representative Liability’ and Recital 80

95. All of the above, in my view, and taking the fullest and most rounded perspective of the scheme of the GDPR and the other aids to interpretation available, would comfortably have led to the conclusion for which the Defendant contends. It is a contextualised, functional, practical and positive analysis in support of that conclusion. Notwithstanding the Claimant’s arguments that none of it absolutely excludes his interpretation, the absence of positive support for that in the places one would look for it, and the contrary indications of intention to exclude it, do not in my view add up to a persuasive case for ‘representative liability’.
96. The best positive support for it is, however, Rec.80. Up until the last sentence of the Recital, its text is in my view fully conformable to, consistent with and supportive of the analysis set out above, and positively advances no different or problematic proposition. The final sentence is, however, a challenge: *‘The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.’* It has to be read alongside Art.27.5: *‘The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.’* Does that mean that these two sentences should be reconciled by deducing that ‘without prejudice to’ in Art.27.5 means joint and several ‘representative liability’ as the best way of accommodating the ‘subject to’ of Rec.80? Does it mean by analogy with *Blanche v EasyJet* that any possible ambiguity about whether Art.27.5 creates ‘representative liability’ must be resolved in the affirmative?
97. My starting point is that, properly contextualised and for all the reasons set out above, Art.27 is not ambiguous about whether it requires that a representative stand in the shoes of a controller as a respondent/defendant to enforcement action: it does not create ‘representative liability’. The fact that Art.27 may not absolutely exclude the Claimant’s contended interpretation does not make it ambiguous.

Approved Judgment

98. If there *were* any ambiguity about Art.27, I would not find *Blanche v EasyJet* an appropriate analogy. In that case, a recital was deployed to give detail to a concept clearly articulated in the operative text ('extraordinary circumstances'). That is not this case. Again, for the reasons set out above, it seems to me that the Claimant's argument seeks to use a recital to cantilever into the operative text an entire system of liability for which it has not, or not sufficiently, visibly provided. It is too slender a basis to bear the considerable weight he seeks to place on it.
99. In any event, it is not beyond debate what 'subject to' means in Rec.80. Read alongside the original consultation text of the EDPB Guidelines it might have been thought tolerably clear: it meant '*the intention to enable enforcers to initiate enforcement action against a representative in the same way as against controllers or processors. This includes the possibility to impose administrative fines and penalties and to hold representatives liable.*' Read alongside the final EDPB Guidelines, 'subject to enforcement proceedings' can be understood to mean subject to the possibility '*for supervisory authorities to initiate enforcement proceedings through the representative*', including '*the possibility for supervisory authorities to address corrective measures ... imposed on the controller ... to the representative*' (that is, an obligation to accept service of process).
100. Rec.80 must be read as a whole, and can no more be taken out of context than any other provision in the complex and interconnected system of the GDPR. The EDPB Guidelines expressly reference Rec.80 in what they say about the obligations and responsibilities of representatives: they have it clearly in view. Without speculating about the historical development of these provisions, 'representative liability', at any rate so far as concerns the relationship between national regulators and representatives, may have been a live policy idea at some point, the last sentence of Rec.80 and the first draft of the EDPB Guidelines being high watermarks of a policy tide which receded. That it *has* receded appears from the Guidelines and the ICO's position.
101. I find no positive encouragement for 'representative liability' anywhere other than the last sentence of Rec.80. I find no strong compulsion there. If I did, then in all of the circumstances rehearsed in this analysis I would in the end have found ample justification for two simple conclusions: that if the GDPR had intended to achieve 'representative liability' then it would necessarily have said so more clearly in its operative provisions; and that it is a proposition on any basis too weighty to be blown in by the 'interpretative sidewind' of the last sentence of Rec.80.
102. In these circumstances, my conclusion is that the interpretation of Art.27 contended for by the Claimant is over-extended and under-supported, and that contended for by the Defendant is to be preferred as more consistent with the letter and spirit of the GDPR.

Conclusion

103. For the reasons given, I find no basis in law for this claim to be brought against the Defendant, in its capacity as the Art.27 representative of WorldCo. The claim is accordingly struck out.