



Neutral Citation Number: [2021] EWCA Civ 800

Appeal No: C1/2019/2726/QBACF

**IN THE COURT OF APPEAL (CIVIL DIVISION)**  
**ON APPEAL FROM THE HIGH COURT OF JUSTICE**  
**QUEEN'S BENCH DIVISION**  
**ADMINISTRATIVE COURT**

**Mr Justice Supperstone**  
**[2019] EWHC 2562 (Admin)**

Royal Courts of Justice  
Strand, London, WC2A 2LL

Date: 26/05/2021

**Before:**  
**LORD JUSTICE UNDERHILL**  
**(Vice-President of the Court of Appeal (Civil Division))**  
**LORD JUSTICE SINGH**  
and  
**LORD JUSTICE WARBY**

**Between:**  
**The Queen on the application of**  
**(1) The Open Rights Group**  
**(2) the3million**

**Appellants/  
Claimants**

**- and -**

**(1) The Secretary of State for the Home Department**  
**(2) The Secretary of State for Digital, Culture, Media  
and Sport**

**Respondents/  
Defendants**

**- and -**

**(1) Liberty**  
**(2) The Information Commissioner**

**Interveners**

**Ben Jaffey QC and Julianne Kerr Morrison (instructed by Leigh Day) for the Appellants**  
**Sir James Eadie QC and Tristan Jones (instructed by the Treasury Solicitor) for the  
Respondents**

**The First Intervener was not represented**  
**Christopher Knight (instructed by ICO) for the Second Intervener**

Hearing dates: 24-25 February 2021

**Approved Judgment**

*Covid-19 Protocol: This judgment was handed down remotely by circulation to the parties' representatives by email, release to BAILII and publication on the Courts and Tribunals Judiciary website. The date and time for hand-down is deemed to be 10:00am on 26 May 2021.*

## **Lord Justice Warby:**

### **Introduction**

1. This appeal is concerned with the lawfulness of statutory restrictions on data protection rights, in the context of immigration. By paragraph 4 of Schedule 2 to the Data Protection Act 2018 (“DPA 2018”) Parliament enacted “the Immigration Exemption”. This disapplies some data protection rights where their application would be likely to prejudice immigration control.
2. The first appellant is a digital rights organisation that seeks to promote and uphold privacy and data protection rights. The second appellant is a grassroots organisation of EU citizens resident in the UK. On 24 August 2018, the appellants brought a judicial review claim against the Secretaries of State for the Home Department and Digital, Culture, Media and Sport, seeking a declaration that the Immigration Exemption was unlawful and an order disapplying it. The main grounds of challenge were that the Immigration Exemption was incompatible with the General Data Protection Regulation (“GDPR”) and/or with the Charter of Fundamental Rights of the European Union of 7 December 2000 (“the Charter”); accordingly, by virtue of the principle of supremacy of EU law, the Exemption could not stand. The respondents denied both these contentions.
3. The claim was heard by Supperstone J and dismissed by him for reasons set out in his judgment of 3 October 2019, [2019] EWHC 2562 (Admin). Permission to appeal was granted by my Lord, Singh LJ, on 14 November 2019.
4. The main issue in the appeal is whether the Immigration Exemption is non-compliant with Article 23 of the GDPR, the provision that authorises an exemption of this kind. For the reasons and to the extent set out below, I have concluded that it is, and that the appeal should therefore be allowed. This makes it unnecessary to address the appellants’ additional contention that the Immigration Exemption is incompatible with Articles 7, 8 and 52 of the Charter (privacy, data protection and scope of guaranteed rights).

### **The Legal Framework**

#### *The GDPR*

5. The GDPR (Regulation (EU) 2016/679) is EU legislation that is directly applicable in all EU Member States. It entered into force on 24 May 2016, and applied with effect from 25 May 2018. The UK is no longer a Member State, but Parliament has decided to keep substantially the same regime in place: see [12-13] below.
6. The GDPR enacts a number of data protection rights and obligations that are now familiar in general terms, as they were contained in the predecessor legislation, the Data Protection Directive 95/46/EC (“the Directive”) and given effect in the UK via the Data Protection Act 1998 (“DPA 1998”). The GDPR also adds some new rights that were not expressly included in the Directive or DPA 1998, including the right to erasure or “right to be forgotten”.

7. The provisions that are relevant for present purposes are contained in Articles 5, 13-15, 17 and 21. Article 5 is contained in Chapter II (Principles). It sets out the six data protection principles, known for short as (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy; (e) storage limitation; and (f) integrity and confidentiality. The other relevant Articles are contained in Chapter III (Rights). Articles 13 and 14 prescribe the information to be provided to a data subject when collecting personal data that relates to them. Article 15 confers the right of access by the data subject, who is entitled to obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and certain specified information about the processing. It also contains provision for the data subject to be given information about safeguards for data transfers to third countries, that is to say, countries outside the EU. Article 17 confers the right to have the controller erase personal data in specified circumstances. By Article 18, data subjects are given the right to have the controller restrict processing in specified circumstances. Article 21 confers a qualified right for the data subject to object “on grounds relating to his or her particular situation”, to certain kinds of processing of personal data. These include processing, the lawful basis for which is that it is “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller” (Article 6(1)(e)).
8. The GDPR contains a number of express exceptions to the rights it confers. None of these is directly relevant. We are concerned with Article 23, which authorises Member States to enact further exceptions. Article 23 is headed "Restrictions" and provides, so far as material, as follows:

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

- (a) ...;
- (b) ...;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest ..., in particular an important economic or financial interest ....., including monetary, budgetary and taxation matters, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;

- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
  - (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
  - (i) the protection of the data subject or the rights and freedoms of others;
  - (j) the enforcement of civil law claims.
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least where relevant as to:
- (a) the purposes of the processing or categories of processing;
  - (b) the categories of personal data;
  - (c) the scope of the restrictions introduced;
  - (d) the safeguards to prevent abuse or unlawful access or transfer;
  - (e) the specification of the controller or categories of controllers;
  - (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
  - (g) the risks to the rights and freedoms of data subjects; and
  - (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction."

*The DPA 2018*

9. The Immigration Exemption was enacted in purported compliance with Article 23. It came into effect, with the rest of the DPA 2018, on 23 May 2018. Paragraph 4 of Part 1 of Schedule 2 provides:

"(1) The GDPR provisions listed in sub-paragraph (2) do not apply to personal data processed for any of the following purposes—

- (a) the maintenance of effective immigration control, or
- (b) the investigation or detection of activities that would undermine the maintenance of effective immigration control,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b).

(2) The GDPR provisions referred to in sub-paragraph (1) are the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—

- (a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);
- (b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);
- (c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
- (d) Article 17(1) and (2) (right to erasure);
- (e) Article 18(1) (restriction of processing);
- (f) Article 21(1) (objections to processing);
- (g) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (f).

(That is, the listed GDPR provisions other than Article 16 (right to rectification), Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing) and Article 20(1) and (2) (right to data portability) and, subject to sub-paragraph (2)(g) of this paragraph, the provisions of Article 5 listed in paragraph 1(b).)

(3) Sub-paragraph (4) applies where—

- (a) personal data is processed by a person ('Controller 1'), and
- (b) another person ('Controller 2') obtains the data from Controller 1 for any of the purposes mentioned in sub-paragraph (1)(a) and (b) and processes it for any of those purposes.

(4) Controller 1 is exempt from the obligations in the following provisions of the GDPR—

- (a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),
- (b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),
- (c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and
- (d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c), to the same extent that Controller 2 is exempt from those obligations by virtue of sub-paragraph (1).”

10. This was a new provision. Nothing of this kind was to be found in the DPA 1998.

*The principle of supremacy of EU law*

11. It is a fundamental principle of EU law that where the law of a Member State is inconsistent with EU law, it is the latter that prevails. If and to the extent that a domestic

provision cannot be read in such a way as to comply with the EU legislation, it should be disapplied. The principles were articulated by this court in *Benkharbouche v Embassy of Sudan* [2015] EWCA Civ 33, [2016] QB 347 [69-85]. *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003 shows this process at work in the context of data protection.

### Brexit

12. The appellants' challenge to the Immigration Exemption was launched on 24 August 2018, when the UK was still an EU Member State. The claimants' case relied on the principle of supremacy of EU law. The claim was tried, and judgment was given, after "exit day", 29 March 2019, but during the implementation period provided for by the withdrawal agreement. That period ended on 31 December 2020 ("IP completion day"). We heard the appeal in February 2021. But it is common ground that the UK's withdrawal from the EU has not materially affected the position.

(1) Sections 2, 3 and 6 of the European Union (Withdrawal) Act 2018 ("EUWA") provided for certain aspects of EU law to remain in force, as part of English law, notwithstanding withdrawal. This is known as "retained EU law". The GDPR, DPA 2018, and relevant CJEU case-law pre-dating IP completion day all fell into this category.

(2) By section 5(2) of EUWA, the principle of the supremacy of EU law continues to apply "so far as relevant to the interpretation, disapplication or quashing of any enactment... passed or made before exit day". What this means is explained in paragraph 103 of the Explanatory Notes:-

"Where ... a conflict arises between pre-exit domestic legislation and retained EU law, subsection (2) provides that the principle of the supremacy of EU law will, where relevant, continue to apply as it did before exit. So, for example, a retained EU regulation would take precedence over pre-exit domestic legislation that is inconsistent with it."

The Immigration Exemption is "pre-exit domestic legislation".

(3) A statutory instrument of 2019 made amendments to the GDPR and DPA 2018 with effect from IP completion day.<sup>1</sup> As a result the GDPR, as it applies domestically, is now known as "the UK GDPR". But the UK GDPR has the same legal status today as the GDPR had before IP completion day. Article 23 is now in slightly amended terms, but the amendments are not material. In Article 23(1), references to "the Union" and "Member State" are deleted and the power to restrict is now conferred on the Secretary of State. There is no change to Article 23(2). The Immigration Exemption is unamended.

13. The respondents accept that in these circumstances the Court could in principle make a declaration that the Immigration Exemption is contrary to Article 23 of the GDPR and Article 23 of the UK GDPR. They also accept that, in principle, the Court would also

---

<sup>1</sup> See The Data Protection, Privacy and Electronic Communications (Amendments, etc) (EU Exit) Regulations 2019 (SI 2019/419).

have the power to disapply the Immigration Exemption if it finds that provision to be incompatible with Article 23 of the UK GDPR.

### **Aspects of the evidence**

14. The claimants adduced evidence via a witness statement of Luke Piper, an immigration solicitor and legal advisor to the second claimant. The respondents submitted evidence from Alison Samedi, Deputy Director of Compliance and Enforcement Policy, and thus the senior Home Office civil servant responsible for data protection policy in relation to the Border, Immigration and Citizenship System (“BICS”). She explained why the Exemption had been introduced, and how it operated in practice, giving some illustrative examples.
15. It is unnecessary to refer to this evidence in detail, but I should note four features. First, the exhibits to Mr Piper’s statement include ostensibly authoritative reports that cast doubt on the accuracy and reliability of the Home Office decision-making in the arena of immigration and data protection. In 2016, a review for the Independent Chief Inspector of Borders and Immigration found that in 10% of cases where a search of the Home Office database identified an individual as a “disqualified person” who should be refused a bank account, the answer was wrong. There were also mistaken omissions. The evidence is that in the second quarter of 2017, the success rate for appeals against Home Office immigration decisions was 47%. The fact that the Home Office dealt imperfectly with “the Windrush Generation” is a matter of common knowledge.
16. Secondly, it is clear that the Immigration Exemption plays a significant role in practice as a brake on access to personal data. Ms Samedi’s evidence is that in the first year of operation of the DPA 2018 the Home Office received 27,984 new subject access requests relating to the BICS, of which 18,332 were progressed for response by a caseworker. The Immigration Exemption was relied on in 10,823 cases, that is to say 59% of responses. The Exemption is available in principle in a wide range of other situations.
17. Thirdly, there is some evidence as to the decision-making methodology of the Home Office, when applying the Exemption. Ms Samedi refers to a dip sampling and assurance exercise in respect of 100 Home Office decisions. This found that the Exemption had “not been used to redact personal information in a blanket way”. Ms Samedi’s evidence is that case workers applied “the prejudice test”, concluding that compliance with the request for subject access was likely to prejudice the maintenance of effective immigration control, and considered that this outweighed the benefits to the individual exercising their data subject rights. In the majority of cases, the Exemption was used to redact small amounts of information, and this was mostly information relating to the “Warnings Index”. This is a Home Office system that “provides the capability to query a database of biographical information about persons, documents and organisations that may be of interest to the Department and other public authorities”. Ms Samedi says that confirmation that an individual has or does not have a record on this Index may facilitate circumvention of border controls, and thereby undermine border security.
18. Finally, there is the guidance that is and may become available to decision-makers. Ms Samedi explains that Home Office decisions are made with the benefit of “draft internal guidance” prepared by policy officials within the BICS Policy and International Group,

and published internally on the Home Office intranet. This guidance has been revised in the light of the claimants' submissions in the present case. It has not been finalised, says Ms Samedì, because it concerns new legislation which needs to 'bed in', and the Home Office wishes to await statutory guidance which it understands the ICO intends to issue. The ICO has published some guidance on the Immigration Exemption. On 10 February 2020, she placed on her website specific guidance on this topic, as part of her more general guidance on the GDPR. This was done in the performance of the ICO's general function of promoting public awareness and understanding of issues relating to the processing of personal data, conferred by Article 57(1)(b) of the GDPR. In that sense, it is statutory guidance. But this guidance does not have any formal, legal effect; the statutory scheme does not require any person to have regard to this guidance, still less to comply with it.

### The judgment below

19. Supperstone J held that the Immigration Exemption fell within GDPR Article 23(1)(e) as it was plainly a matter of "important public interest" and pursued a legitimate aim. Contrary to the arguments advanced by the appellants and supported by Liberty, the first intervener, the Exemption was in accordance with the law. The state was not required to demonstrate that the measure itself was "strictly necessary". The CJEU authorities relied on in support of that proposition were cases where the legislation itself constituted or required an interference with individual rights. The issue here was what the law requires "where the legislation does not itself create or require interference with the data rights of individuals but instead makes abstract provision for an exemption which may be relied on by data controllers if they can justify doing so in the circumstances of a particular case." In such a case, the decision on whether the measure is necessary was in principle a matter for the state, in respect of which a margin of appreciation applies. It was not necessary for the legislative measure itself to prescribe where it applies, and to contain all the relevant safeguards. It was reasonable for Parliament to have enacted the Immigration Exemption, applying the appropriate margin of appreciation.
20. The Judge held that the criteria by which to test the lawfulness of the measure were to be found in the decision of the Supreme Court in *The Christian Institute v The Lord Advocate (Scotland)* [2016] UKSC 51 [79-81] ("*Christian Institute*"), and in *In Re Gallagher* [2019] 2 WLR 509 [41] (Lord Sumption). The Immigration Exemption satisfied those criteria as it was "comprehensible", it did not suffer from any lack of clarity or foreseeability, and there was an adequate set of safeguards to protect individual data subject rights. The Immigration Exemption could only be relied on if and to the extent that compliance with the relevant GDPR provisions "would be likely to prejudice" the specified public interest purposes, and the Exemption could only be applied where that was necessary and proportionate. Case law made clear that in this context the state must demonstrate "a very significant and weighty chance of prejudice" to the relevant public interest: *R (Lord) v Secretary of State for the Home Department* [2003] EWHC 2073 (Admin) [100] (Munby J). The test of necessity was strict: *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 6443 (QB) [45]. The requirement of proportionality did not need to be specified in the Immigration Exemption as it was implicit in the necessity test, and set out in terms in the GDPR. In addition, the GDPR/DPA 2018 regime provided safeguards in the form of an enforcement regime, affording a legal remedy and judicial protection.

21. The Judge also rejected the appellants' submission that in any event the Immigration Exemption did not comply with the specific requirements of Articles 23(2)(a)–(h). In the light of what he had said earlier, he did so relatively shortly. He held that the Exemption complied with the requirements of Articles 23(2)(a)–(c), because the provisions setting out the purposes for which, and the categories of data to which, it may be applied were “clear and appropriately delineated”. As for the safeguards required by Article 23(2)(d), there was no need for these to be specified in the Exemption itself. When considering whether there are sufficient safeguards the Court “can look not only at formal legislation but also at published official guidance and codes of conduct”: *Christian Institute* [81]. The same applied to Articles 23(2)(g) and (h) (risks and notification) because “notification rights are provided for elsewhere in the legislation”. There was nothing objectionable about the fact that the Exemption could be relied on by any data controller that decided its processing fell within paragraph 4(1), including – for instance – private landlords. So Article 23(2)(e) was not contravened.
22. The Judge rejected the argument of the Information Commissioner (“ICO”) that although the Immigration Exemption was in accordance with the law, and could “in principle” be lawful, it would not be a proportionate implementation of Article 23 in the absence of accompanying statutory guidance to provide safeguards as to its meaning and application. The Judge held that a legislative measure does not need to be accompanied by guidance as to proportionality in order to be lawful. He considered the reasoning in *Christian Institute* provided no support for the ICO’s submission. The decision in that case did not turn on considerations of proportionality but on whether the legislation under scrutiny was “in accordance with the law” for the purposes of Article 8 ECHR. Additional guidance was only required in that case because, in its absence, the primary legislation was so unclear that it failed that test. That was not the position here.

### Issues on the appeal

23. The appellants advance what in substance are two main points. First, they contend that the Judge was wrong in law to hold that the legal requirements for a lawful derogation differ according to whether the legislation itself creates or requires interference with individual rights, or instead permits or authorises the use of an exemption by data controllers in particular cases. It is submitted this distinction is inconsistent with the decision of the CJEU’s Grand Chamber in *Tele2 Sverige AB and Watson (Joined Cases C-203/15 & C-698/15)* [2017] 2 CMLR 30 (“*Tele 2*”), and unsupported by any CJEU authority. The Judge should have followed *Tele 2*, and applied a test of strict necessity. The test he did apply, of whether the legislation could be operated lawfully, is inapplicable to legislation such as this, which removes or restricts a right (“derogation cases”). That test only applies to cases where legislation involves an interference with rights which requires justification (“justification cases”).
24. Secondly, it is said that the Judge was wrong to approach the case by reference to principles applicable to Article 8 ECHR. The relevant CJEU jurisprudence, and the terms of Article 23(2) itself, make clear that the circumstances in which a derogation such as the Immigration Exemption will apply, and under what substantive and procedural safeguards, must be clearly prescribed by the legislation itself and/or appropriate guidance with the force of law. The Judge was wrong to approach the case on the footing that these matters could lawfully be dealt with in other ways.

25. Much of the appellants' argument focuses on this second ground of appeal. The skeleton argument of Mr Jaffey QC and Ms Kerr Morrison put the appellants' "essential complaint" in this way: "the Immigration Exemption is so-over broad as to be in breach of the express requirements governing derogations in Article 23(2) of the GDPR and the CJEU's strict caselaw providing protection for data rights against attempts [to apply] generally worded derogations."
26. For the ICO, Mr Knight supports the appellants' position that the relevant test is one of strict necessity, and challenges the Judge's conclusion on proportionality. He repeats the submission that without guidance carrying statutory force the Exemption is a disproportionate interference with fundamental rights. He submits that the authorities show that the nature and extent of any safeguards are matters to be considered not only at the stage when the court is considering whether a measure is in accordance with the law, but also when proportionality is under scrutiny. He emphasises the importance of the rights at stake and the sensitivity of the context. He submits that the conclusion to be drawn from Article 23 and the relevant jurisprudence is that, in the present context, the requirement of proportionality can only be met by the safeguard of formal guidance with statutory status. By that he means guidance with which data controllers are legally required to comply, or to which they are legally obliged to have regard, or which a court or tribunal is bound to take into account.
27. For the respondents, Sir James Eadie QC and Mr Jones support the Judge's decision, and his legal analysis. They characterise the Immigration Exemption as a "permissive" measure. They submit that the CJEU cases relied on by the appellants do not establish that a test of strict necessity applies to measures of that kind. The correct approach was explained in *Christian Institute*: the legislature's decision that such a measure is necessary may only be impugned if unreasonable; the measure will be proportionate if it is capable of being operated in all or most cases without giving rise to an unjustified interference with Article 8; it must be in accordance with the law, which includes a requirement for relevant safeguards against abuse. The Immigration Exemption satisfies these requirements.
28. It is further submitted that Article 23(2) contains a checklist of matters that are not legally irrelevant, but amounts to no more than a list of topics. Those topics do not need to be dealt with in the derogating legislation itself, or in tailored guidance with legal force; they can all properly be dealt with in any part of domestic law. The law contains a suite of relevant safeguards including the applicable provisions of the GDPR itself, DPA 2018, and the Human Rights Act 1998. These deal adequately with each of the topics specified in Article 23(2), so far as those are relevant here, with the consequence that the Exemption "falls comfortably within what is permitted by Article 23(2)". To make good this submission, Sir James has taken us through each of the specified topics, identifying legal provisions that - in his submission - provided the necessary safeguards. Thus, for example, the requirement for "specific provisions ... as to ... safeguards to prevent abuse" in Article 23(2)(d) is said to be met by controls contained in the DPA 2018, Article 58 of the GDPR (powers of the domestic supervisory authorities) and other enforcement mechanisms. It is said that if the requirement for "specific provisions ... as to ... the storage periods ..." is relevant at all, it is met by Article 5(1)(e) of the GDPR.

## Discussion

29. The argument has been wide-ranging but I would suggest that, if my Lords agree, this appeal can and should be decided on the following short and straightforward basis. There presently exists no legislative measure that contains specific provisions in accordance with the mandatory requirements of Article 23(2) of the GDPR. In the absence of any such measure, the Immigration Exemption is an unauthorised derogation from the fundamental rights conferred by the GDPR, and therefore incompatible with the Regulation. For that reason, it is unlawful. The appeal succeeds on this aspect of Ground 2, and it is unnecessary to reach conclusions on the other issues raised.

### The text of the GDPR

30. It is helpful to start with the text of Article 23. Article 23(1) has a familiar structure. It authorises a restriction on the scope of certain specified obligations and rights if it is done “by way of a legislative measure”, “respects the essence of the fundamental rights and freedoms”, and is a “necessary and proportionate measure in a democratic society to safeguard” one of the specified aims, purposes, or objectives. This structure broadly reflects the way in which the Charter and the European Convention on Human Rights define the conditions under which the state can legitimately interfere with a qualified fundamental right.
31. It is to be noted, however, that the function of Article 23 is different. Whereas Article 8 of the Convention (for instance) prescribes the conditions under which a state interference with the right to respect for private and family life, home and correspondence may be justified, Article 23 is a measure which permits the state to restrict the very scope of the right, including by removing it from the citizen altogether, in the specified circumstances. This is a distinction on which Mr Jaffey has placed considerable reliance. He categorises, and seeks to contrast, the two situations as legislative “justification” and legislative “derogation”. Mr Knight supports this analysis.
32. The language and structure of Article 23(2) are not familiar from the Charter or the Convention. Nor is any comparable provision to be found in the Data Protection Directive. This is new. It is, by common consent, a provision that particularises the requirements of Article 23(1). That is clear from the opening words. As is also obvious, Article 23(2) sets out details of what a “legislative measure” must do, if it is to comply with the more broadly stated requirements of Article 23(1). The legislative measure has to “contain specific provisions” about the eight listed matters “at least, where relevant”. As a matter of grammar, and on a natural reading, this would seem to mean that the legislative measure must at least include specific provision about each of the eight listed matters, where or to the extent that the listed matter in question is relevant; it may need to include specific provision about other matters as well.
33. Putting this another way, it seems to me that on the face of it Article 23(2) contains a condition precedent to the validity of any “legislative measure” purporting to fall within Article 23(1): the measure can only satisfy the requirements of Article 23(1) if it contains specific provision as to each matter that (a) is listed in Article 23(2) and (b) is, in the circumstances, relevant to an assessment of whether the measure (i) respects the essence of the right in question and is (ii) necessary and proportionate for one or more

of the listed purposes or objectives. The language clearly suggests that the legislative measure must have some binding force.

34. If that is right, then this all seems to be a logical and explicable scheme. As Mr Knight put it on behalf of the ICO, the natural reading of the wording used is that the legislator sees the specification required by Article 23(2) as a way of securing the proportionality required by Article 23(1). As I have indicated at [33] above, the purpose of Article 23(2) may, to my mind, go beyond that, but Mr Knight's submission neatly encapsulates the point about the structure of Article 23 as a whole.
35. The Recitals to the GDPR provide some context and some help in understanding the language adopted. Recital (6) records that "rapid technological developments and globalisation have brought new challenges for the protection of personal data." Recital (7) records that "Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced." Recital (41) explains the notion of "legislative measure" for the purposes of the GDPR:

"Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights."

In this case, we are not concerned with a reference to a "legal basis". The term used is "legislative measure" which would seem to be something narrower. There is a degree of flexibility in the concept. It evidently need not be primary legislation, but clearly it must be something that qualifies as "legislative" in some sense. And whatever it is, it must be clear, precise and its application must be foreseeable. Those would seem to be requirements of the "legal certainty" mentioned in Recital (7). We are directed by Recital (41) to look to the case-law for the content of these requirements.

#### The European cases

36. The relevant case-law of the CJEU includes five decisions of the Grand Chamber to which we have been referred. They are *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* [2014] 3 CMLR 44 ("Digital Rights Ireland"); *Tele2* (above); *EU-Canada Passenger Name Record (PNR) Agreement* [2018] 1 CMLR 36 ("Opinion 1/15"); *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (Case C-623/17) ("Privacy International"); and *La Quadrature du Net and others* (Cases C-511/18, C-512/18 and C-520/18) ("La Quadrature"). In my judgment, this body of jurisprudence, progressively built up over the years, justifies several of the headline submissions of Mr Jaffey. I would accept that the cases show that the CJEU has been alert to the risk of over-broad derogations from fundamental rights; requires any derogation from fundamental rights to be justified by proof of strict necessity; and does not consider that this, or the requirement of

proportionality, can be satisfied unless the appropriate safeguards are built into the legislative measure.

37. This all serves to buttress the provisional conclusions at which I arrived by considering the language of the GDPR. I would accept Mr Jaffey's further submission, that the language of the Regulation reflects principles to be found in the developing CJEU jurisprudence. I cannot detect in these cases any support for the submission of Sir James Eadie, and the conclusion of the Judge, that a distinction is to be drawn between different kinds of derogation, and that different criteria apply to a derogation that is "permissive".
38. In *Digital Rights Ireland*, the applicants challenged the lawfulness of amendments to Article 15 of Directive 2002/58 ("the e-Privacy Directive") effected by Article 5 of Directive 2006/24 ("the Data Retention Directive"), and domestic legislation implementing these measures, which required telecommunications companies to retain traffic and location data for a specified period. The purpose was to combat crime. The Grand Chamber recognised this as a legitimate aim, but held that Article 5 represented a derogation from fundamental rights which exceeded the limits of proportionate interference with articles 7, 8 and 52 of the Charter. The Directive was to that extent invalid.
39. The e-Privacy Directive authorised the adoption of "legislative measures to restrict the scope of the rights and obligations" provided for by the Directive, including measures for "the retention of data for a limited period", if such measures were "a necessary, appropriate and proportionate measure within a democratic society to safeguard ... the prevention, investigation, detection and prosecution of criminal offences ... [and] in accordance with the general principles of Community law". The Court held that the seriousness of the interferences involved called for "strict review", and the importance of the rights at stake meant that any derogations should apply "only insofar as strictly necessary": [48], [52]. At [54] the Court spelled out the consequence:

"... the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."

The Data Retention Directive failed that test because the wide-ranging and serious interference which it entailed was not "precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary": [65]. Among other things, the Directive failed to lay down any objective criterion to ensure that access to and use of the retained data by the state was limited to "that which is strictly necessary in the light of the objective pursued"; or any mechanism for achieving this, or any specific obligation on Member States to establish such limits ([61-62]); the data retention periods were too broadly defined, without reference to the different categories of data ([63]); and there were no rules to ensure the security and protection of retained data ([66]), or its retention within the EU ([68]).

40. In *Tele2* the Grand Chamber considered two conjoined cases about the compatibility of domestic legislation with the Data Retention Directive, read in conjunction with

Articles 7 and 8 of the Charter, and in the light of *Digital Rights Ireland*. The UK legislation at issue was the Data Retention and Investigatory Powers Act 2014 (“DRIPA”). Section 1 of DRIPA empowered the Secretary of State to serve a notice requiring a telecommunications operator to retain relevant communications data “if the Secretary of State considers that the requirement is necessary and proportionate” for one of certain specified purposes. The Secretary of State was given power to make regulations about the retention of data. The questions referred by this Court included whether *Digital Rights Ireland* laid down “mandatory requirements of EU law applicable to a Member State’s domestic regime...” The Grand Chamber answered in the affirmative, holding as follows (emphasis added):-

“116 .... As regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure, in accordance with what was stated at [95] and [96] of this judgment, that such access does not exceed the limits of what is strictly necessary.

117 Further, since the legislative measures referred to in art.15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, “be subject to adequate safeguards”, *a data retention measure must, as follows from the case law cited at [109] of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.*

118 In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in art.15(1) of Directive 2002/58, even if that objective is to fight serious crime. That *national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data* (see, by analogy, in relation to Directive 2006/24, the Digital Rights [2014] 3 C.M.L.R. 44 at [61]).”

41. *Opinion 1/15* was about a draft agreement between the EU and Canada (“the draft Agreement”) on the transfer and processing of Passenger Name Record (“PNR”) data. The European Parliament asked the Court for a binding opinion on the compatibility of the draft Agreement with the Charter and the Treaty on the Functioning of the European Union (“TFEU”). The draft Agreement contained several internal safeguards, and some provision for administrative and judicial oversight. The UK and other governments supported the contention of the Council and the Commission that the case was

distinguishable from *Digital Rights Ireland*, and the agreement was compatible. The Grand Chamber concluded that the draft Agreement was incompatible with the Charter in several respects, among them its failure to lay down clear and precise provisions governing the PNR data to be transferred; criteria to ensure that the data was processed exclusively for the fight against terrorism and serious transnational crime, in a way that was reliable and non-discriminatory; and limits on the data to be retained and the length of its retention. The Court said (emphasis added, and omitting internal citations):

“139 ... the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that *the legal basis which permits the interference with those rights must itself define the scope of the limitation* on the exercise of the right concerned ...

140 As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case law of the Court, that derogations from and limitations on the protection of personal data should apply only insofar as is strictly necessary ....

141 In order to satisfy that requirement, *the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards*, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. *It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted*, thereby ensuring that the interference is limited to what is strictly necessary.”

42. I note at this point that s 1 of DRIPA was a provision which did not in itself interfere with the ordinary rights of data subjects, but authorised the Secretary of State to abrogate certain of those rights where he considered this necessary for national security purposes. Article 4(1) of the draft Agreement between the EU and Canada provided that “The European Union shall ensure that air carriers are not prevented from transferring PNR data to the Canadian Competent Authority ...”. So in these respects at least the draft Agreement could be viewed as containing “permissive” provisions for derogation.
43. The same is true – perhaps more obviously – when it comes to the legislative provisions considered by the Grand Chamber in *Privacy International*. Section 94 of the Telecommunications Act 1984 authorised the Secretary of State to give directions to the Office of Communications (“OFCOM”) and providers of public telecommunications networks, if the Secretary of State considered this “necessary in the interests of national security” or certain other interests. Section 94(1) authorised “such directions of a general character as appear to the Secretary of State to be necessary”. Section 94(2) authorised the Secretary of State to direct such a person “to do, or not to do, a particular thing specified in the direction”. Section 94(2A) provided that the Secretary of State should not give any such direction “unless he believes that

the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.” In practice, these powers had been used to compel telecoms companies to provide the security services with a live feed of their data, to allow bulk interrogation and searches of the data.

44. In proceedings against the Foreign Secretary, Home Secretary, and others the Grand Chamber was asked for a preliminary ruling on the compatibility of these provisions with EU law. It ruled that national legislation enabling a state authority to call for the “general and indiscriminate transmission” of data to the security and intelligence services was precluded by Article 15 of the e-Privacy Directive, read in the light of Article 4(2) TFEU and Articles 7, 8, 11 and 52 of the Charter. At [65-68], the Court reiterated the principles identified in the passages from *Digital Rights Ireland* and *Opinion 1/15* that I have cited above. At [76] it held that national legislation entailing interference with Articles 7 and 8 of the Charter must comply with those requirements “in order to satisfy the requirement of proportionality ... according to which derogations from and limitations on the protection of personal data must apply only in so far as strictly necessary ...”. The Court went on, at [77], to say this:-

“In particular, as regards an authority’s access to personal data, legislation cannot confine itself to requiring that authorities’ access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use ...”

There are distinct echoes here of the language of Article 23(2) of the GDPR.

45. The fifth and last in this list of Grand Chamber decisions, *La Quadrature*, was another preliminary ruling. Again, the Court was asked to consider the interpretation and application of the e-Privacy Directive in the context of domestic legislation requiring data retention. The decision was delivered on the same day as *Privacy International*, and the overall approach and conclusion were to similar effect. At [130], discussing Article 15, the Court reiterated the requirement of “strict necessity” for any derogation from the protection of personal data. At [132], it recalled the requirement for clear and precise rules, imposing minimum safeguards and sufficient guarantees against abuse, holding that the legislation must be “legally binding ...and, in particular, must indicate in what circumstances and under what conditions a measure ... may be adopted.” The Court held that the Directive precludes legislation that provides for the general and indiscriminate retention of traffic and location data as a precautionary or preventive measure. Thus far, the Court’s approach is familiar from the jurisprudence already cited.
46. But *La Quadrature* is unique in this sequence as it also addressed the provisions of the GDPR. It did so in the context of a question referred by the French Conseil d’Etat in Case C-512/18, as to whether Directive 2000/31/EC (“the e-Commerce Directive”) was applicable, and permitted the state to introduce legislation of the kind in question: see [73(2)]. The Court ruled that this was not the case, as the e-Commerce Directive itself provided that it was not to apply to questions about information society services that were covered by the Data Protection Directive: [199]. The governing law was to be found in Article 15(1) of the e-Privacy Directive or, since the repeal of the Data Protection Directive, Article 23 of the GDPR: [200-202]. The Court drew a close parallel between the two provisions, holding that the same approach applies:-

“209. Article 23(1) [GDPR] much like Article 15(1) of [the e-Privacy] Directive 2002/58 ... allows Member States to restrict, for the purposes of the objectives that it provides for and by means of legislative measures, the scope of the obligations and rights that are referred to therein ‘when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard’ the objective pursued. Any legislative measure adopted on that basis must, in particular, comply with the specific requirements set out in Article 23(2) of that regulation.

210. Accordingly, Article 23(1) and (2) [GDPR] cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein ... In particular, as is the case for Article 15(1) of [the e-Privacy] Directive ... the power conferred on Member States by Article 23(1) ... may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary ...

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

47. These authorities seem to me to lend considerable support to the appellants’ first Ground of Appeal ([23] above). There is clearly some overlap or interplay between the notions of necessity and proportionality as deployed in these decisions. In this jurisprudence the two notions, treated as distinct in the Strasbourg jurisprudence, permeate and colour one another. But one clear and consistent theme is that derogations in this area must be justified as strictly necessary. There is no trace of any doctrine that a less exacting standard of review may apply where the relevant legislation does not itself involve an abrogation or interference, but merely authorises it. As I have said, on a fair analysis, at least two of the cases involve what would seem clearly to be “permissive” provisions for derogation. Nor is it easy to accept Sir James Eadie’s submission that these cases can be explained and distinguished on the footing that context is the key, and that these cases, unlike the Immigration Exemption, involved interferences that were wide-ranging and particularly serious. For my part, I am not persuaded that the domestic cases on which the Judge relied – which I shall deal with briefly later - provide support for his analysis.
48. As I have indicated, however, I would prefer to decide this case on a narrower basis. I do not believe Article 23 should be construed as merely requiring the state to provide a general legal framework that contains guarantees of necessity and proportionality, and other safeguards. That might be a legitimate interpretation of Article 23(1), if it stood alone. But our analysis must reflect the fact that when updating and strengthening EU data protection law in the GDPR the legislature chose to depart from the approach to derogation that it had adopted in Article 13 of the Data Protection Directive. It particularised the requirements of Article 23(1), at some length, and in some detail, in

Article 23(2). It seems to me that the respondents' argument fails to explain or account for this and, in the process, leaves Article 23(2) with no significant purpose or function. In one sense, Article 23(2) clearly does provide a checklist. But I do not consider it plausible that Article 23(2) was intended to amount to nothing more than a sort of high-level aide-memoire to the state about the kinds of matters it should have in mind when deciding whether to derogate from fundamental rights, in pursuit of one of the specified aims. The checklist is cast in mandatory terms, and calls for "specific" provisions. Sir James's submission that these "specific provisions" can be found in general principles of human rights or administrative law, or in existing Articles of the GDPR is unconvincing. Article 23(2) itself – on the face of it – requires them to be contained in "any legislative measure referred to in paragraph 1".

49. It may be that this wording is not to be read entirely literally; but it is remarkably specific and surely must be given some meaning. At any rate, in my judgment the better view, in the light of the CJEU jurisprudence, is that Article 23(2) requires any derogation to be effected by a "legislative measure" that is tailored to the derogation, legally enforceable, and contains provisions that are specific to the listed topics - to the extent these are relevant to the derogation in question - precise, and produce a reasonably foreseeable outcome. It can, I think, be said that this interpretation follows from the CJEU decision in *La Quadrature*. As I read that decision, the Court adopted and applied in the context of Article 23 of the GDPR the body of jurisprudence it had built up over the preceding years when dealing with Article 15 of the e-Privacy Directive and the Data Retention Directive. More generally, in this respect the Luxembourg jurisprudence and the language of Article 23(2) seem to me to be broadly if not precisely in step. The CJEU has repeatedly rejected submissions to the effect that domestic legislation should be held to pass muster on the basis that sufficient safeguards could be found elsewhere in the overall legal framework. The language of Article 23(2) seems to me to reflect the lines of reasoning enunciated in *Digital Rights Ireland* [54] and *Tele2* [117-118], and the legislature may properly be considered to have intended an outcome on the same lines.
50. The essence of the reasoning, as I see it, is that broad legal provisions, such as those that require a measure to be necessary and proportionate in pursuit of a legitimate aim, are insufficient to protect the individual against the risk of unlawful abrogation of fundamental rights. The legal framework will not provide the citizen with sufficient guarantees that any derogation will be strictly necessary and proportionate to the aim in view, unless the legislature has taken the time to direct its attention to the specific impacts which the derogation would have, to consider whether any tailored provisions are required and, if so, to lay them down with precision. This approach will tend to make the scope and operation of a derogation more transparent, improve the quality of decision-making, and facilitate review of its proportionality. To my mind the evidence to date as to the relevant decision-making tends to emphasise the importance of characteristics such as these.

The EDPB Guidelines, 2020

51. I have reached these conclusions by reference to the language of Article 23 and the CJEU jurisprudence, but I am comforted to note that they are consistent with paragraphs 45-46 of the *Guidelines 10/2020 on restrictions under Article 23 GDPR* published by the European Data Protection Board ("EDPB"). The EDPB is a body established under Article 68 of the GDPR with the task of ensuring consistent application of the

Regulation; the Guidelines are published in pursuit of that objective: see Article 70(1)(e). Paragraph 45 of the Guidelines says that "... any legislative measure adopted on the basis of Article 23(1) GDPR must, in particular, comply with the specific requirements set out in Article 23(2) ... As a rule, all the requirements detailed below should be included in the legislative measure imposing restrictions ...". Paragraph 46 suggests that any exceptions to this rule, based on the fact that one or more of the provisions of Article 23(2) is not relevant, "need to be duly justified by the legislator". The Guidelines were adopted on 15 December 2020, after the decision of the Judge, but before exit day.

### The United Kingdom cases

52. None of the domestic cases cited here or below bears directly on the proper interpretation of Article 23(2). But I would make brief reference to three Supreme Court cases, in date order: *South Lanarkshire v Scottish Information Commissioner* [2013] UKSC 55, [2013] 1 WLR 2421; *Christian Institute*; and *R (Hemmati) v Secretary of State for the Home Department* [2019] UKSC 56, [2021] AC 143.
- (1) Unlike the Judge, I regard *South Lanarkshire* as to some degree supportive of the appellants' case that a different approach is to be taken to measures that interfere with a fundamental right and those that derogate from, restrict or disapply the right. The case itself was about the former category, but Baroness Hale recognised the distinction that Mr Jaffey advocates, observing that it was "well established in Community law that, *at least in the context of justification rather than derogation*, 'necessary' means 'reasonably' rather than absolutely or strictly necessary": [27] (emphasis added). This was perhaps prescient. The case was decided before the line of CJEU decisions discussed above. But those cases bear out the distinction drawn by Lady Hale, and show that a test of strict necessity is applied in Community law, when it comes to derogations.
  - (2) *Christian Institute* I would class as a justification case. The relevant issue, for present purposes, was whether the measures under scrutiny were "incompatible with any of the Convention rights or with EU law", the allegation being of a breach of the Article 8 rights of parents: [26], [67]. So I would disagree with the Judge. *Christian Institute* is not authority that the claimant challenging a derogation such as the Immigration Exemption faces the "high hurdle" of having to show that the provision is incapable of being operated in a manner compatible with Convention Rights.
  - (3) In *Hemmati* – decided after the judgment of Supperstone J in this case - the Supreme Court adopted an approach that bears close comparison with that of the CJEU in the cases cited, albeit in a different legal context. The "Dublin III" Regulation (604/2013) provided that the detention of a person subject to its procedures had to comply with strict safeguards, including clarity, predictability and accessibility. The Court held that this required national law to define objective criteria, in a binding provision of general application, which set out the limits of the flexibility allowed to the authorities in assessing individual cases, and was foreseeable in its application. The Secretary of State's detention policy fell short.

### The Immigration Exemption

53. I would agree with the Judge that the Immigration Exemption addresses an important aspect of the public interest, that falls within the scope of Article 23(1)(e). But I have concluded that he was wrong to reject the appellants' submissions as to Article 23(2) and instead to apply the *Christian Institute* approach. On my reading of Article 23 as a whole, it seems clear that the Immigration Exemption is non-compliant. The Exemption itself contains nothing, specific or otherwise, about any of the matters listed in Article 23(2). Even assuming, without deciding, that it is permissible for the "specific provisions" required by Article 23(2) to be contained in some separate legislative measure, there is no such measure. It has not been suggested that the draft internal guidance produced by the Home Office qualifies as such. The ICO's present guidance is doubtless of some value, but it is somewhat vague and, critically, it does not have the force of law. Its provisions might be a relevant consideration for a public law decision-maker, as Sir James Eadie submits, but I am not at all persuaded that this would be enough to comply with Article 23(2). It is not to be forgotten that the Immigration Exemption applies to a range of private bodies and individuals. In any event, the term "legislative measure", whatever its precise scope, must refer to something other than a non-binding code promulgated by a regulator that counts as a relevant consideration for the purposes of administrative decision-making.
54. I have indicated a provisional view that the legislative measure in question must be part and parcel of the legislation that creates the derogation, but I do not think that this is the point at which to decide what form the "specific provisions" should take. I merely note Mr Knight's observation that, on the face of it, s 16 of the DPA 2018 confers wide-ranging powers on the respondents to vary the terms of provisions made under Schedule 2. It is certainly not for us to prescribe the content of any of the specific provisions which the Regulation requires. It may be open to the legislature to conclude that one or more of the matters listed in Article 23(2) is not relevant to this particular exemption. It may even be entitled to conclude that although a particular matter is relevant it is unnecessary to set limits any narrower than those contained in the GDPR itself. But that is not the way the respondents have put their case at this stage. The reason there are no specific provisions is not that the legislature has gone through any reasoning process of this kind. On the contrary, the respondents' stance has been consistent throughout: that as a matter of principle no such process is required, as it is enough for individual decisions to comply with the general requirements of the GDPR itself, extraneous legislation such as the Human Rights Act, and other measures of legal control. That stance, in my judgment, is legally wrong.

### **Disposal**

55. The claim form seeks a declaration that the Immigration Exemption is incompatible with the Charter and the GDPR, and an order that it be disapplied, or alternatively a more limited form of declaration, specifying the conditions under which the Exemption might be lawfully applied. But at the conclusion of the hearing it was common ground that if we were in favour of the appellants the question of what relief should follow our decision would need to be the subject of separate argument. Mr Jaffey expressly invited us to take a step-by-step approach. Sir James suggested that if the case got to this point there would need to be an opportunity to put in evidence. He pointed to the confirmation in *La Quadrature* at [215-219] that domestic courts do have some limited

power to allow the temporary suspension of the ousting effect of a rule of EU law which is found to be inconsistent with national law.

56. The appropriate remedy in a case of incompatibility is a sensitive matter, that may depend on the nature of the incompatibility identified by the Court: see the decision of the Divisional Court in *R (Liberty) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin), [2020] 1 WLR 243 [87-90], [391] (Singh LJ and Holgate J). Here, I have identified an omission that is, in principle, capable of remedy by measures that amend or supplement the existing provision. In the circumstances, I see merit in the cautious approach of both sides. I would defer a decision on relief, inviting further submissions on that issue in the light of these reasons.

**Lord Justice Singh:-**

57. I agree.

**Lord Justice Underhill:-**

58. I also agree.