IN THE HIGH COURT OF JUSTICE KING'S BENCH DIVISION [2023] EWHC 2653 (KB)

MEDIA AND COMMUNICATIONS LIST

Claim No. QB-2022-000433

BETWEEN:-

MR BORIS KARPICHKOV

Respondent/Claimant

-and-

THE NATIONAL CRIME AGENCY

Applicant/Defendant

JUDGMENT

Counsel for the Applicant/Defendant: James Cornwell instructed by Messrs. Weightmans solicitors.

Counsel for the Respondent/Claimant: Eric Metcalfe instructed by Messrs. Deighton Pierce Glynn solicitors.

List of UK Statutory Sources referred to in argument or in judgment

Extradition Act 2003

Data Protection Act 2018

List of EU and other International Sources referred to in argument or in judgment

Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. (CETS No. 108)

The Charter of Fundamental Rights of the European Union Document 2012 2012/C 326/02

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States ("the Framework Decision").

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) ("The SIS II Decision")

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data (the Law Enforcement Directive ("LED")).

Commission Notice — Handbook on how to issue and execute a European arrest warrant 2017/C 335/01

List of ECHR Provisions referred to in argument or in judgment

Art. 3

Art. 6

Art. 8

List of Authorities referred to in argument or in judgment

Hollington v F Hewthorn & Co [1943] KB 587

Barrett v LB Enfield [2001] 2 AC 550 at 557

Swain v Hillman [2001] 1 All ER 91

ED & F Man Liquid Products v Patel [2003] EWCA Civ 472

Hughes & Ors v Richards [2004] EWCA Civ 266

McKennitt v Ash [2006] EWCA Civ 1714, [2008] QB 73

Easyair Ltd v Opal Telecom Ltd [2009] EWHC 339 (Ch)

South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55

AB v A Chief Constable [2014] EWHC 1965 (QB)

Rogers v Hoyle [2014] EWCA Civ 257, [2015] QB 265

Guriev v Community Safety Development (UK) Ltd [2016] EWHC 643

Oysterware Ltd v Intentor Ltd & Ors [2018] EWHC 611

Cooper v National Crime Agency [2019] EWCA Civ 16

Elgizouli v Secretary of State for the Home Department [2020] UKSC 10

Driver v CPS [2022] EWHC 2500 (KB)

C-88/22 Opinion of Advocate General Emiliou in Regionų apygardos administracinio teismo Kauno rūmai, delivered on 7 July 2022

Textbooks referred to in argument or in judgment

Phipson on Evidence (20th ed., 2021)

List of abbreviations

DPA – Data Protection Act 2018

DPPs – Data Protection Principles

EAW – European Arrest Warrant

ECHR – European Convention on Human Rights and Fundamental Freedoms

ECtHR – European Court of Human Rights

FSB - Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii

GDPR – General Data Protection Regulation

KGB - Komitet Gosudarstvennoy Bezopasnosti

LED – Law Enforcement Directive

LSP - Latvian Security Police

MPI – Misuse of Private Information

NCA – National Criminal Agency

SOCA – Serious Organised Crime Agency

SIRENE - Supplementary Information Request at National Entities

SIS II – Schengen Information System II

SSHD – Secretary of State for the Home Department

SVR - Sluzhba vneshney razvedki Rossiyskoy Federatsii

Accessible language summary. This simplified summary is not part of the judgment but must be reproduced with it. It has a Flesch-Kincaid reading ease score in excess of 50.

This case concerns the Claimant who was formerly known as Mr Karpichkov. He now has a new identity. For present purposes he is accepted as being a former KGB double agent. He worked within the Latvian security services and also the Russian security services. He is now a British Citizen. Details of his new name and address in the UK were disclosed to the Latvian authorities by the Defendant. He alleges he has received death threats in his new identity at his new address. Fuller facts appear at the start of the judgment.

I directed at a previous hearing that disclosure which tends to reveal the current name or address of the Claimant must not be reported in the press or otherwise be made public. This judgment does not contain any such information and is 'OPEN'. There is no 'CLOSED' judgment.

A British court in the past has ruled that the Claimant is:

> *"… in a unique position to confirm past collaboration by high-ranking Latvian officials with the KGB. He is also likely to be considered a threat to the Russian intelligence services by virtue of his work as a double agent for the Latvian LSP and against Russian state interests and by his on-going outspoken criticism of Russia. … [his] life has been at risk since these allegations were first brought …".*

The events here took place before "Brexit", when the UK was a full EU member. The legal issues relate closely to the cooperation arrangements then in place between the UK and other EU states.. Those arrangements related among other things to the European Arrest Warrant system.

The Claimant says that the National Crime Agency as the UK's Competent Authority wrongly disclosed his new identity to the Latvian State 'SIRENE' Bureau on 23 July 2018 and also disclosed his UK address on 22 May 2019. 'SIRENE' stands for "*Supplementary information request at national entities*". How that system operates is set out in this judgment because it is central to this case. SIRENE is a form of EU inter-country cooperation whereby information is shared between EU law enforcement agencies, for example relating to suspects wanted for crimes.

The Claimant says that as a result of the disclosures by the NCA the Russian State has gained knowledge of his new identity and address and this has resulted in threats written in Russian delivered to his new home. He has described himself as '*a dead man walking*' in the media, where he has some profile in the UK under his former identity.

The Defendant is the National Crime Agency. Its is a part of the UK State. It argues that it had to disclose the new name and address of the Claimant by virtue of law governing exchange of information between EU states relating to criminal suspects. What it did cannot in its view in principle be said to be unlawful under any data protection rights within the UK's Data Protection Act 2018, or at common law. In short the Defendant claims to have a complete defence.

The Claimant says that the UK State need not have given the disclosure and that the law provides a more nuanced position than argued for by the State. In the Claimant's view the UK State failed to weigh the balance of those UK provisions relative to the EU's data sharing arrangements.

The analysis I reach is somewhat different from either party's analysis, albeit the Claimant is the successful party. The judgment provides my full reasons but my conclusion for the purposes of this

summary can be shortly stated. It is arguable that the Defendant should have considered whether the disclosures in this case were truly 'required' by the applicable law once one took into account Human Rights and EU Charter provisions given the factual background specific to this case.

If disclosure would be contrary to fundamental rights then in my judgment it would not be strictly 'required' under Art 1(2)(b) of the EU Law Enforcement Directive by EU or Member State Law. The Executing Authority would then arguably be obliged to apply the domestic UK law in the form of the Data Protection Act's Data Protection Principles. It could impose restrictions or refuse the transfer of data either outright or unless modified to protect fundamental rights. One could not simply say it had met all required legal criteria such as 'necessity' merely by following European Arrest Warrant and Schengen Information system processes if a breach of fundamental rights would mean that transmission was not lawfully required.

A full understanding of this judgment can only be gained from reading it. This summary however is intended to ensure that the outcome and core basis is clear, namely that subject to any appeal Mr Karpichkov's case can proceed.

Contents

*Note: In this decision unless stated otherwise any emphasis in the text such as **bold** or <u>underlined</u> text is my own. Quotations are in italics.*

[1] Although many of the points made here were presented prior to oral argument by C, it is convenient to treat them in logical sequence after C's argument in this decision.

Introduction

1. This case concerns a person who for present purposes is accepted as being a former KGB (later FSB) double agent, who worked within the Latvian security services as well as working for the Russian security services and who is a British Citizen. Details of his new name and address in the UK were disclosed to the Latvian authorities by the Defendant.
2. He alleges he has received death threats in his new identity and at his new address. He also alleges that in 2006-7 (before the disclosures forming part of this case) he may have also been the victim of a possible chemical or biological attempt on his life.
3. I directed at the hearing that disclosure of any details which tend to reveal the current name or address of the Claimant must not be reported in the press or otherwise be made public. This judgment does not contain any such information and is 'OPEN'. There is no 'CLOSED' judgment.
4. A British court in the past (details below) has ruled that the Claimant ("C") is:

   "… in a unique position to confirm past collaboration by high-ranking Latvian officials with the KGB. He is also likely to be considered a threat to the Russian intelligence services by virtue of his work as a double agent for the Latvian LSP and against Russian state interests and by his on-going outspoken criticism of Russia. … [his] life has been at risk since these allegations were first brought …".

5. It is common knowledge that law enforcement agencies in the UK take the view – and the ECtHR[2] so found - that the Russian State via its officers killed former KGB officer Alexander Litvinenko in 2006 and also that the Russian State stands accused of attempting to murder former KGB agent Sergei Skripal and his daughter in Salisbury in 2018, both of which events likely only serve to reinforce Mr Karpichkov's concerns.
6. Measures were taken by myself and staff in this case to protect any disclosure of his current details such that any relevant documents were secured within the

[2] European Court of Human Rights

Royal Courts of Justice, however C was able to attend the hearing before me with his legal representatives.

7. This judgment necessarily delves deeply into EU and domestic legal provisions. My decision and reasons are given in Part V which may be read first by those seeking a more rapid understanding.

Apparent facts

8. The events here took place before "Brexit" had entered its 'implementation period' and the UK was a full EU member. Hence the legal issues relate closely to the cooperation arrangements then in place between the UK and other EU states when the UK was a part of the EU. It may be that similar arrangements remain today, after Brexit, but this decision does not need to go into that.

9. I take this general chronology from a document prepared at my request which was not wholly agreed, but nothing turns on the dates here and nor do I need to make findings. Mr Karpichkov (not his current name) is a former Soviet KGB officer holding the rank of Major who worked for the Russian State as an agent for that country, and was recruited in 1984 into the Latvian KGB section.
10. In May 1990 Latvia declared independence from the Union of Soviet Socialist Republics and in September 1991 C began working in Latvia as an undercover agent for the FSB (Russian Intelligence, the successor to the KGB).
11. He ceased to work for the FSB in January 1995, instead from May that year working undercover for the LSP (Latvian security service). He was arrested in 1996 by the Latvian authorities but exited to Moscow the next year, where he claims to have been interrogated by the FSB and tortured.
12. In July 1997 he then began working as an undercover agent for the LSP (Latvia) in Russia. That November he returned to Latvia and went into hiding there, hiding from the Latvian authorities.
13. He moved to Britain in 1998 as an asylum seeker together with his immediate family. In December 1998 he and his family changed their names by way of Statutory Declaration. His family likewise adopted new identities for their protection. C notified the Home Office of his new identity and his reasons for

adopting it. He also took steps to ensure that his addresses in the UK were not publicly known. That said, under his old identity he publicised unlawful activity by the Russian and Latvian intelligence services on an ongoing basis.

The Claim

14. C before me alleges that the Defendant, the National Crime Agency (henceforth "D") as the UK's Competent Authority wrongly disclosed his current identity to the Latvian State (in particular by disclosing information the Latvian 'SIRENE' Bureau about which more later) on 23 July 2018 and then later also disclosed his UK address via the same channel, on 22 May 2019.

15. 'SIRENE' stands for "*Supplementary information request at national entities*"[3]. I shall describe how that system operates later in this judgment because it is central to this case. SIRENE is a species of EU inter-country cooperation whereby information is shared between EU law enforcement agencies, *inter alia* relating to suspects wanted for crimes, not very dissimilar to the European Judicial Network which operates at a judicial level and with which this author is more familiar after judicial training some years ago in the context of war crimes and crimes against humanity[4].

16. C alleges that as a result of the allegedly unlawful disclosures above, the Russian State has gained knowledge of his new identity and address and that this has resulted in threats, in Russian, delivered to his new home and that his life is at risk. He has described himself as '*a dead man walking*' in the media, where he has some profile in the UK which can readily be found under his former identity on the internet, but not in his new identity.

17. C's claim is for:

- damages for breach by D of the 1st, 3rd and 6th Data Protection Principles ("DPPs") under the Data Protection Act 2018 ("DPA") (ss.35, 37 and 40); and/or

[3] https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_en

[4] https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN

- damages for misuse by D of his private information.

In a nutshell

18. In perhaps over-simplified form but for aid of understanding, the parties' positions might be characterised thus:

    D, an emanation of the UK State, argues that it was obliged by law to disclose the current name and address of C by virtue of law governing exchange of information relating to criminal suspects. What it did cannot therefore be said to be unlawful under any data protection rights within the UK's DPA 2018, or at common law.

    C on the other hand says that the UK State need not have given the disclosure in question and that the law provides a more nuanced position than contended for by D. For C, the UK State had failed to weigh the balance of those provisions relative to the EU's prosecutorial data sharing arrangements.

    The analysis I reach by way of conclusion is somewhat different from either party's analysis, albeit the Claimant is the successful party.

The extradition and arrest warrant history

19. As the history below will show, the fact that Latvia is now an EU state has not prevented a very troubling history between Latvia's legal and judicial system and C, which resulted in an adverse ruling by the court in this country concerning illegitimate efforts to extradite him back to Latvia.

The first extradition request by Latvia

20. On 11 October 1999, at a time when Latvia was not a member of the EU (and in any event the European Arrest Warrant system had not yet been put in place) the Latvian authorities sought to extradite C on the basis of various criminal allegations. That November, the Home Office commenced the process to extradite him back to Latvia. On 19 July 2001, the Home Office refused C's asylum claim but granted him exceptional leave to remain on grounds of his risk of ill-

treatment contrary to Art 3 ECHR if returned to Latvia and in December of 2001 the Home Office agreed to process new travel documents in C's new name[5].

21. On 12 June 2002, the High Court agreed to quash the Home Office's extradition decision because the Secretary of State accepted that it would be "wrong, unjust or oppressive" for C to be extradited, since he would be in danger of his life from "underworld/rogue government elements if he were returned or extradited".

The First European Arrest Warrant from Latvia

22. Notwithstanding the previous refusal of the UK State to extradite C, on 6 December 2007, Judge Buls of the Riga District Court issued a European Arrest Warrant ('the 2007 EAW') for C's arrest and extradition. That EAW was accompanied by an 'alert' to the UK authorities on the SIS II system (discussed later). On 18 June 2008 the Secretary of State for the Home Department ("SSHD") granted C indefinite leave to remain. This did not end the EAW process, however. On 14 October 2009, the Serious Organised Crime Agency ("SOCA") certified the 2007 EAW and sent it to the Metropolitan Police the same day.

British Citizenship granted to C

23 On 19 July 2010, C was granted British citizenship. The details on his naturalisation certificate were those of his new, British, identity. On 5 August 2010, he was issued a British passport.

The Second Extradition Request by Latvia

24. On 27 March 2018, the Latvian authorities issued a request via SIRENE asking authorities to "*perform checks*" in their databases for details of C's whereabouts "*in order to establish the wp's*[6] *whereabouts with the view to extradition*". That request was repeated in April that year, now stating that he was "*wanted by the Serious Crimes Department of the General Prosecutor's Office of Latvia for forgery*

[5] Article 3 - Prohibition of torture: No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

[6] Ie 'wanted person'

of documents and misappropriation in a large scale". The Latvian authorities observed that he was "*well known in the UK as public person Boris Karpichkov"* and asked the UK to *"provide us information about the wanted person*".

The Home Office's view of the Second Extradition Request

25. On 6 May 2018, the Home Office notified D that C was living under his new British identity and was a naturalised British citizen and D was already aware of the previous grant of leave to remain on human rights grounds. The Home Office informed D that given C was now a British Citizen the 'leave to remain' based on human rights would no longer apply (ie effectively the basis for him being in the UK was his right as a citizen and not by way merely of permission).
26. D in turn advised the Kent Police – who would be the body actually arresting C if an arrest were to take place – that, although the alleged offences forming the basis of the second extradition request were the same as those relating to the refused first request, there was in law no bar to extradition inasmuch as the human rights position of this (now) British Citizen would be considered as part of the extradition process in the normal way for a British Citizen.
27. Kent Police decided not to execute the EAW given that the 1999 extradition request had been refused on human rights grounds (an unsurprising decision given that the alleged offences were is seems the same as the basis for the original request).
28. On 19 June 2018, D notified Kent Police, tersely and perhaps indicating some difference of opinion, that there was "*currently no bar to [C's] extradition*" and that Kent police's decision not to execute the EAW on human rights grounds was based on outdated information, and was "*entirely your decision and should [C] re-offend in the UK, the responsibility lies with yourselves*".

The Disclosure of C's new name by D to Latvia

29. On 23 July 2018, D provided the Latvian authorities with details of C's new British identity but not his address. Latvia also wanted to know his address. However D asked the Latvian authorities to "*please advise the reason as to why you would require an address for the subject?*"

30. After July 2018, C says he began to receive anonymous threats referring to his British identity and intimating that his UK address was known to them. I do not need to make any findings about this or who the sender(s) may have been or exactly when or how the Russian authorities obtained the information, if they obtained it at all (which is in issue).

31. On 13 September 2018, the Latvian authorities among other things asked D for confirmation that C *"is known and was identified by your authorities as [NAME] as the wanted person under his real name gave interviews to the UK mass media .... Additionally we would like to know his address if he is the same person for whom we searching for, because our competent authority to take proper legal actions in the criminal case".*

32. On 19 October 2018, Kent Police arrested C pursuant to the 2007 warrant. C counsel's submission at hearing was that a form G, required by SIRENE, was sent to the Latvian authorities which stated under the heading, "Circumstances surrounding the hit", that "*Officers attended the subjects address and arrested him on the EAW*". The address was <u>not</u> stated and C relied in part on this as being said to show that inclusion of the address could not be seen as 'necessary'.

33. Some significant time – 40 days – after the hearing I received a witness statement from Ms Browne of D which indicated that that form G was in fact <u>not</u> provided to the Latvian authorities but had been drafted, and it could only be speculated why it was not sent via SIRENE to Latvia, but that it may have been related to the Magistrates' Court having released Mr Karpichkov that day and released the EAW.

34. C strongly objects to the statement being admitted very late in evidence and in any case argues both that it is technically defective and that it highlights not only issues with the record keeping of D and its disclosure but also that, if one were to take it at face value, it shows it was quite possible for D if it chose, to have omitted to include address details in a form G.

35. I do not feel that the evidence if admitted would add anything to my decision or affect my reasons given later and will not admit it in evidence in the light of the objections. It is I think in any case self-evident that a form G could be prepared – whether or not served - which textually omitted details, and the fact of its service or non-service on Latvia does not materially affect my legal analysis later in this

judgment since an incomplete form G would be as consistent with a mistaken failure to comply with the rules as to the exercise of a legitimate discretion to omit details, or it would be consistent with this possibly unserved form G being a draft. It is not a matter for me to have to decide today.

36. On the same date, 19 October 2019 Kent Police emailed HM Courts and Tribunal Service notifying them of C's pending court appearance. Among other things, it stated that C "has been arrested in his current legal name of [**NAME**])". C was discharged and released from custody on the basis that he was not "brought as soon as practicable before the appropriate judge", i.e. before the Westminster Magistrates' Court, as required by section 4(3) of the 2003 Extradition Act.

Latvia tries again: the Second European Arrest Warrant, and official disclosure of C's address

37. On 2 November 2018, the Latvian authorities (SIRENE Latvia) repeated their request for details of C's UK address, referring to the UK news media in relation to him stating publicly he had been arrested and stating the information was wanted "*as it will helps to our competent authority to take further actions*" (sic) and that, with the police here were being '*humiliated*' and that the '*excellent work*' of the police was being '*put down*' by the Claimant in the media. On 20 and 27 February 2019, C and one of his sons allege that they received anonymous letters containing death threats.

38. On 4 April 2019, the Latvian authorities issued a second EAW and on this occasion stated, in the Warrant, C's new name. On 21 May 2019, C was arrested, and D notified the Latvian authorities of C's arrest on a form G on 22 May.

39. It was at this point that D also disclosed to them C's UK home address using "form G" referred to in the SIS II Decision and SIRENE Manuals. There were also direct communications between D and the Latvian SIRENE bureau.

"An abundance of dangerous enemies": The UK court prevents surrender of C to Latvia

40. On 1 September 2020, District Judge Baraitser refused extradition under the Second Arrest Warrant because:

(i) the extradition request was in fact issued for the purpose of prosecuting or punishing C for his political opinions, contrary to s13(a) of the Extradition Act 2003;

(ii) there was cogent evidence in C's case to displace the ordinary presumption that he would receive a fair trial if returned to Latvia;

(iii) it would be unjust or oppressive to extradite him by reason of the passage of time; and

(iv) it would be incompatible with his right to a fair trial under art 6 ECHR.

41. Judge Baraitser accepted that there was evidence "*to support [C's] claims that he ... has dangerous enemies in Russia who would wish for his silence*" and that C faced a real risk of harm from Russian and Latvian elements. The learned judge noted that the Home Office had already accepted that C's life was at risk including from "*rogue government elements in Latvia*" when the Secretary of State had originally decided to grant him Exceptional Leave to Remain in the UK. The judge noted that C was a threat to the Latvian government:

"not least by being in a unique position to confirm past collaboration by high-ranking Latvian officials with the KGB. He is also likely to be considered a threat to the Russian intelligence services by virtue of his work as a double agent for the Latvian LSP and against Russian state interests and by his on-going outspoken criticism of Russia. I am satisfied that he has received recent death threats likely to have emanated from Russia ....

I accept that [C's] life has been at risk since these allegations were first brought [in the 1990s]. When he left Latvia, it was as an FSB double agent, with an abundance of dangerous enemies in both Latvia and Russia. Although nearly three decades have passed since he left Latvia, the threat to his life has remained, evidenced most recently by two 'death threat letters' likely to have been sent to him by agents of the Russian state. In my view, [C] has remained beyond the reaches of the Judicial Authority in order to keep himself safe and I consider his circumstances to be of the most exceptional kind..."

This Claim: procedural history

42. On 1 July 2021, C sent D a letter of claim, alleging breach of his data protection rights and misuse of his private information. D provided a substantive response to the letter before claim on 8 November 2021. After an agreed extension of time, on 10 February 2022, C issued the claim and on 6 April 2022, D filed and served its defence. Prior to the claim, D had declined to offer protection to C arising from the alleged threats.

43. I allocated C's claim to the Multi-track. The present application now before me was issued on 27 February 2023. I directed C to file and serve his Reply to D's application along with any evidence by 12 April 2023, and that D's application be listed for hearing.

The application

44. The NCA applies by application dated 27 February 2023 to strike out the Claim and/or for Summary Judgment.

45. D admits that it made the disclosures referred to above. Its position is that it was obliged to disclose the relevant information to the Latvian Bureau under the package of EU legislation governing European Arrest Warrants and the sharing of information between EU judicial authorities.

46. In this judgment there is little sensible alternative than to set out the details of the statutory provisions and related material which underpin the regulation of disclosures in the course of communication between EU States operating law enforcement between SIRENE bureaux. Those appear in the Annex to this judgment but are also quoted in the body of the judgment where particularly relevant.

47. There is nothing between the parties as to the legal framework itself but where the parties differ is as to whether, as D claims, it was <u>obliged</u> to make the disclosures which it did or whether it had discretion or flexibility as to what was disclosed and hence could have taken more care over revealing the personal data relating to C's new name and address. For the sake of precision, C puts the scope of the legal dispute thus:

"To the extent that there is any dispute between the parties as to the relevant legal Framework … it concerns the extent to which D's obligations to provide information under the Framework legislation is subsidiary to its obligation to process C's personal data in accordance with the Data Protection Principles as set out in Chapter 2 to Part 3 DPA and Art 4 LED and, more generally, C's rights under articles 7 and 8 of the EU Charter of Fundamental Rights[7]"

[7] Which effectively incorporates the ECHR though if there is any relevant difference I shall mention it (my note).

Part I - The law on striking out and summary judgment

48. I need only briefly set out the applicable law as to the circumstances in which this court may terminate some or all of a claim. I set it out because it is probable that non-lawyers will read this decision. I have taken this uncontroversial summary from the D's skeleton argument merely for convenience.

CPR r.3.4 provides:

*"**3.4 Power to strike out a statement of case***

...

(2) The court may strike out a statement of case if it appears to the court—

(a) that the statement of case discloses no reasonable grounds for bringing ... the claim; ..."

49. A claim may be struck out under CPR r.3.4(2)(a) if, *inter alia*, it is incoherent, makes no sense, and/or raises no recognisable claim (i.e., a claim that is not valid as a matter of law) (CPR PD 3A, para. 1.4)).

50. CPR r.24.2 provides, in material part, that:

"The court may give summary judgment against a claimant ... on the whole of a claim or on a particular issue if—

(a) it considers that—

(i) that claimant has no real prospect of succeeding on the claim or issue; ... ... and

(b) there is no other compelling reason why the case or issue should be disposed of at a trial."

51. The principles applying to summary judgment appear in for example *Easyair Ltd v Opal Telecom Ltd* [2009] EWHC 339 (Ch) at [15] (approved by the Court of Appeal in *A C Ward & Sons Ltd v Catlin (Five) Ltd* [2009] EWCA Civ 1098, [2010] Lloyd's Rep IR 301, per Etherton LJ at [24]) and include:

"i) The court must consider whether the claimant has a "realistic" as opposed to a "fanciful" prospect of success ...;

ii) A "realistic" claim is one that carries some degree of conviction. This means a claim that is more than merely arguable ...;

iii) In reaching its conclusion the court must not conduct a "mini-trial ...;

iv) This does not mean that the court must take at face value and without analysis everything that a claimant says in his statements before the court. In some cases it may be clear that there is no real substance in factual assertions made, particularly if contradicted by contemporaneous documents ...;

v) However, in reaching its conclusion the court must take into account not only the evidence actually placed before it on the application for summary judgment, but also the evidence that can reasonably be expected to be available at trial ...;

vii) ...[I]t is not uncommon for an application under Pt 24 to give rise to a short point of law or construction and, if the court is satisfied that it has before it all the evidence necessary for the proper determination of the question and that the parties have had an adequate opportunity to address it in argument, it should grasp the nettle and decide it. The reason is quite simple: if the respondent's case is bad in law, he will in truth have no real prospect of succeeding on his claim or successfully defending the claim against him, as the case may be. ... However, it is not enough simply to argue that the case should be allowed to go to trial because something may turn up which would have a bearing on the question of construction: ..."

Part II – Defendant/Applicant's argument

Lawful under the EAW and SIRENE provisions

52. For D the key to the case is that the provision of information to the Latvian authorities was regulated by EU law and legal instruments – those cited above – and the "fundamental basis" of the way the EU arrest warrant system operates is on "a high level of confidence between the member states", to quote the 10th recital of the Framework Decision. So not only were the States bound by the relevant EU law, and the provisions of the ECHR as well, but there was an overarching policy that the states involved operated on the 'high confidence level' basis.

53. So, argues D, it was ***required*** to proceed on the basis that the Latvian authorities would act consistently with their obligations under EU law. There was a proper route to deal with concerns relating to legality and human rights protections, which arise from the EAW process, namely the courts of the State (here the UK) executing the warrant. We have seen above that that process operated correctly and prevented his extradition (see para. 40).

54. Here however the issue is disclosure of information in the course of the EAW process prior to the court's decision to prevent extradition. The fact that a subsequent decision was made to discharge the EAW could not, it was said, impugn D's actions in making the disclosures in the first place in the proper course of the EAW process and SIRENE communications.

55. The District Judge who refused extradition by contrast was dealing with consequences to C if he returned to Latvia and that court had no jurisdiction to consider C's safety in the UK per se. That the District Judge gave a decision about risks to C if he returned to Latvia does not (says D) even arguably undermine the legality of D 'merely' exchanging information with the Latvian authorities as part of the SIRENE and EAW processes.

Disclosure was in accordance with the First Data Protection Principle

56. As to the first Data Protection Principle ("DPP") and indeed the other DPPs in the claim D argued that it was plainly correct that the processing of the data relating

to C was 'lawful, necessary and fair' within DPA s.35. Simply: there was an outstanding EAW in 2018 and with it there was an SIS II alert and C, as an international criminal suspect, was still at large, and the SIS II and SIRENE Manual required the disclosures as a matter of law. "*Necessary*" meant on D's submission "*reasonably necessary*", which means than more than merely desirable, but less than indispensable or absolutely necessary (*Cooper v National Crime Agency* [2019] EWCA Civ 16, per Sales LJ at [89-93]). This involved a balancing of the interests of the data subject in non-disclosure (including their reasonable expectations of privacy) against the public interest in disclosure (*AB v A Chief Constable* [2014] EWHC 1965 (QB), per Cranston J at [75]).

57. Any alias that a suspect may be living under was also very relevant information and might even be crucial information enabling them to be located so as to be arrested. Considering the DPA's requirement for 'necessity', those considerations alone showed that it was indeed 'necessary' to process such information.

58. The provisions of EU law were prayed in aid as further confirmation of the undoubted lawfulness of the disclosures. The SIS II Decision and SIRENE Manual governed the process as to disclosure between EU States. Noted especially was the fact that the SIRENE Manual, at 2.12.2 expressly states that: "*Member States shall as far as possible inform each other about aliases ...*"

59. D was, it was said, <u>obliged</u> to inform the Latvian Bureau of the "Alias" Information, ie C's new name. The Alias[8] information was information required by the Framework Decision (Art.8(1)(a)) to be included in an EAW by the Latvian authorities if they had it[9]. [I observe here however that the inclusion of such

[8] In my judgment referring to the Claimant's new name as an alias is strictly incorrect: he had changed his name by Statutory Declaration such that it was no mere alias. UK law does not recognise that a 'birth name' has any particular legal status over later legal names and allows 'self-ID' as to names, by way of use and repute, evidenced generally by a Statutory Declaration and sometimes, albeit rather over-complicatedly, by Deed Poll. Such is the way of the Common Law. His **current** name in my judgment is his **'real'** name. In that respect D says as noted that, *a fortiori*, that therefore is part of the 'indispensable information' which has to be recorded in the SIS II database. In my judgment whether one calls his 'new' name an 'alias' or his 'proper' or 'real' name makes no difference in this case.

[9] "**Content and form of the European arrest warrant**

information in a Warrant *from* Latvia assisting the UK authorities to locate a suspect is not the same thing as disclosure of that information *to* Latvia in response to the Warrant, whilst noting, as does D, that the SIRENE manual does seem to imply a mutual exchange of alias information ('… inform each other …')].

60. Given that C had made a Statutory Declaration in respect of his UK identity on 10 December 1998 it may be that the UK Identity *was* his name and not, strictly, an alias. In which case the above points D says would apply *a fortiori* as such information would qualify as indispensable information (his actual 'real' or 'proper' name) that was to be recorded in the SIS II database. On that basis it would be unnecessary to go as far as considering the interpretation of the provisions of the SIRENE Manual relating to aliases.

61. As to the Address Information, D declined to provide the Address Information to the Latvian Bureau on several occasions. D did then ultimately provide the Address Information, but only as part of the form G reporting his arrest pursuant to the 2019 EAW (the Second warrant) and the accompanying SIS II alert that was disclosed to the Latvian Bureau in May 2019.

62. Under the SIRENE Manual, para. 2.3 (which D says it was required to comply with under Art.8(1) SIS II Decision and para. 1.1 SIRENE Manual) the issuing Member State (i.e. Latvia) is to be informed by the executing Member State (i.e. D) of a "*hit*" and its outcome by way of a form G, which *"... shall provide as much information as possible on the hit...*".

63. The Address Information was provided under "*Circumstances surrounding the hit*" (field 088) and "*Actions taken*" (field 086) in the form G (although it could equally have been provided in the "*Place, date, time the alert was hit*" (field 085). D therefore only provided the Address Information when it was specifically under an obligation to do so as part of giving 'as much information as possible'.

64. The processing of both the Alias and Address Information was thus clearly "*based on law*" for the purposes of s.35(2) DPA 2018 as it was expressly required under

1. The European arrest warrant shall contain the following information set out in accordance with the form contained in the Annex: (a) the identity and nationality of the requested person"

the SIS II Decision and SIRENE Manual. In this context the disclosure of C's Alias and Address Information to the Latvian Bureau was plainly also "*necessary*" for the performance of a task carried out for a law enforcement purpose (as defined in s.31 DPA 2018) by D as a competent authority and as the UK's SIRENE Bureau. If a controller is obliged to do something it must be "necessary", says D.

65. Sections 35(1) and 35 (2)(b) DPA 2018 were, therefore, satisfied and the processing was lawful for the purposes of s.35(1) DPA 2018 as well as being lawful under the SIRENE and EAW legal requirements.

66. Given that D was obliged to provide the Alias and Address Information to the Latvian Bureau it cannot arguably be said that the processing was not also "fair" for the purposes of s.35(1) DPA 2018.

In accordance with the Third Data Protection Principle

67. The complaint in respect of the Third DPP (s.37 of the DPA) also fails inevitably it is said very much for the same reasons as the claim under the First DPP. The Alias and Address Information were information that D was expressly obliged to transmit to the Latvian Bureau. The processing of such personal data by way of such transmission was "adequate, relevant and not excessive" by reference to the law enforcement purposes and D disclosed no more and no less than the information that it was required to disclose acting as a SIRENE Bureau. Aside from simply not providing the Alias or Address Information at all, and departing from what D says it was obliged to provide there was no lesser (i.e., less allegedly "*excessive*") step that D could in principle have taken that would have amounted to compliance with the Third DPP.

In accordance with the Sixth Data Protection Principle (DPA s.40)

68. The Sixth DPP is to the effect that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data. Sections 56-57 and 66 DPA 2018 (which essentially relate to the manner of data handling and security) did not says D materially add anything to C's case. This was not a case of accidental disclosure. The disclosure was a deliberate disclosure (in the case of the Alias Information) in response to a request from the Latvian Bureau and (in respect of both the Alias

and Address Information) consistent with, and pursuant to, D's obligations under the Framework Decision, SIS II Decision and SIRENE Manual. There was no arguably unauthorised or unlawful processing that D was required to safeguard against.

Common law and the Human Rights Act: no misuse of private information

69. D accepts for present purposes that the disclosed information engaged C's rights under Art.8 ECHR[10]. However, the MPI claim fails inevitably according to D because any such privacy rights were outweighed by countervailing interests in the form of those argued in relation to the First DPP namely that the disclosure of the Alias and Address Information to the Latvian Bureau was to comply with D's obligations as the UK's SIRENE Bureau, pursuant to the various EU law instruments, in circumstances where C was a suspect still at large subject to EAWs.

Submission on strike out and summary judgment

70. Given the above, D said that the DPA 2018 claim and the MPI claim lacked merit and the Particulars of Claim disclosed no reasonable grounds for bringing the claim for the purposes of CPR r.3.4(2)(a), and there was 'no real prospect of C succeeding', for the purposes of CPR r.24.2(1)(a)(i).

71. In respect of the second limb of the summary judgment test under CPR r.24.2(b) there was said to be no other compelling reason why the claim (or any part of it) should proceed to trial and the argued fatal deficiencies in C's case are were not likely to be capable of correction by repleading or by way of further evidence

[10] 1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

reasonably likely to be available at a trial. D therefore urged me to strike out the claim or grant summary judgment for D.

Part III – C's response to D's application

72. In a nutshell C says there was no need for D to have disclosed the information which it did. In doing so, it exposed C to a real risk of serious harm or worse. D arguments were said to 'strain both credulity and common sense'. D's obligations to share information with the Latvian authorities were subject at all times to the overriding requirements of EU data protection law and the DPA and the requirement to respect C's fundamental rights under articles 7 and 8 of the EU Charter (and presumably analogous provisions of the ECHR). Nor was D's argument backed by any prior binding authority to demonstrate the contrary.

73. There was said C no basis upon which D could reasonably ask the Court to strike out C's claim, nor to grant Summary Judgment. C's statement of case plainly disclosed reasonable grounds for bringing the claim C, moreover, had a realistic prospect of showing that D breached his data protection rights and/or misused his private information in this case.

Rebutting D's assertion as to the role and effect of the 2002/584/JHA Framework Decision

74. C denied that D was entitled to rely on an argument that the 2002/584/JHA Framework Decision has some form of 'pre-eminence' or that it required D to act as it did in the processing of C's data. It was said C plain that D's obligations under that Framework Decision must be read subject to the requirements of the Law Enforcement Directive ("LED") and the EU Charter itself. This was highlighted especially by Recitals 4, 5, 12 and 40 and Art 1(2) and Art 3(1) of 2008 Framework Decision (repealed and replaced by the LED). These pointed to the significance attached to protection of personal data in the (former) 2008 Framework Decision and carried forward in to the LED.

75. In particular Recital 4 of the (repealed) 2008 Framework decision referred to "*the need for an innovative approach … under the strict observation of key conditions in the area of data protection*". Recital 5 stressed the need for "*clear rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in*

respect of such cooperation between the Member States while fully respecting fundamental rights of individuals". Recital 40 stated that, in relation to the 1981 Convention, where provisions of EU or national legislation imposed "conditions on receiving Member States as to the use or further transfer of personal data are more restrictive than those contained in the corresponding provisions of this Framework Decision, the former provisions should remain unaffected. …".

76. Article 1(2) required Member States to "*protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy*" when sharing data for law enforcement purposes. Article 3(1) provided that *"[p]rocessing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected*".

77. The key role of personal data protection was apparent in the LED which replaced the 2008 Framework Decision. In particular Recital (1) provides materially that the "*protection of natural persons in relation to the processing of personal data is a fundamental right*". Recital (2) states that the "*principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data*". Recital 46 provides that *"[a]ny restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms*". Recital 50 provides, materially, that "*[t]he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to .... loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation*".

78. Article 4(1) LED provides materially, said C, that personal data must be: (a) processed lawfully and fairly; (c) adequate, relevant and not excessive in relation to the purposes for which they are processed and (f) processed in a manner that ensures appropriate security of the personal data.

Case law

79. *Elgizouli v Secretary of State for the Home Department* [2020] UKSC 10 was cited as authority that s76(1) DPA, which requires that a transfer to a third country or international organisation based on special circumstances must be necessary for one of the specified purposes, must be read in light of the recitals to the LED, including the need to respect fundamental rights under Recitals 1 and 46 and the specific requirement in Recital 71 that "*personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment*". See paras. 10-14 of the speech of Lady Hale, para. 157 of the speech of Lord Kerr, paras. 215-217 and 220-226 of the speech of Lord Carnwath.

80. I was referred to *Driver v CPS* [2022] EWHC 2500 (KB), where Julian Knowles J agreed with the submission that there was "*little material distinction between the data protection principles applicable to general processing of personal data in the GDPR and those applicable to processing it for law enforcement purposes in Part 3 of the DPA 2018*" (para 91) and at 109 that the test of '*necessity*' under s35(2) DPA was "*a strict one*". Dicta of Warby J in *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (approved by the Supreme Court in *Elgizouli*) were relied on in *Driver* that "*any interference with the subject's rights ... be proportionate to the gravity of the threat to the public interest*" (para 109). The burden of showing that the disclosure was necessary was on the Defendant (para 114).

81. In *South Lanarkshire Council v Scottish Information Commissioner* [2013] UKSC 55 (a case under the DPA) Lady Justice Hale said that "*the word "necessary" has to be considered in relation to the processing to which it relates. If that processing would involve an interference with the data subject's right to respect for his private life, then the Austrian Radio case is clear authority for the proposition that the requirements of article 8(2) of the European Convention on Human Rights must be fulfilled.*" That case concerned Art. 7(e) of Directive 95/46/EC which was implemented through the DPA 1998, and not Art. 8 of the ECHR. However the case of Mr Karpichkov did by contrast rely on Art. 8 ECHR in the processing of his personal data (see para 43(a) of the Particulars of Claim). Moreover *Elgizouli*

confirmed at SC level more recently that 'necessity' means 'strict necessity' and in doing so applied *Guriev* which was a case in relation to restriction on a subject's rights of access to personal data, indicative of a view that the 'strict necessity' requirement was seen as generally applicable and not to be confined to Third Party data transfers, and quoted Warby J[11].

The requirement to take C's claim at its highest

82. For a strike out application I was reminded that it must be "assumed that the factual basis of C's claim is true" and as far as C was concerned this includes that:

"*a. C was a high-profile defector from the Latvian and Russian intelligence services;*

b. the alleged offences which formed the basis of the Latvian extradition request in 1999, the 2007 EAW and the second EAW in 2019 were false and politically motivated;

c. C was granted Exceptional Leave to Remain by the Home Office on 19 July 2001 on grounds of a real risk of ill-treatment contrary to article 3 ECHR, a risk which arose both from organised criminal elements and rogue governmental elements;

d. that grant of leave was the basis on which the 1999 Latvian extradition request was refused in 2002;

e. C was subsequently granted naturalisation as a British Citizen and a British passport in his British identity rather than his Latvian identity because the Home Office accepted that he had continuing concerns as to his security and that of his family;

f. C continued to receive credible threats from Russian security services and/or other sources since arriving in the UK, including – following D's disclosures – references to his British identity and home address;

g. Kent Police and HM Court Service were each alive to concerns about the risk to C from disclosure of his British identity and home address, as evidenced by the

[11] D points out that the applicability of the strict necessity test did not seem to be in issue in *Elgizouli* as appears from eg para. 210.

email chain dated 19 October 2018 headed "ADVANCE NOTICE of EAW ARRST TOMORROW with complicating/sensitive elements around identity";

h. D itself was alive to concerns about the risk to C from disclosure of his home address, as evidenced by its request to the Latvian authorities on 23 July 2018 for "the reason as to why you would require an address for the subject"; and

i. D knew it was possible to execute an extradition request, including an EAW, without disclosing C's British identity or home address, as evidenced by the fact that no such information was disclosed in the course of the proceedings following the 1999 extradition request nor (in relation to C's home address) the 2007 EAW."[12]

83. I was correctly reminded that I am not obliged, however, to take factual assertions "at face value and without analysis" but C argued that I had been shown no material by way of contradicting contemporaneous material entitling me to disregard the pleaded facts. Rather, C characterised D's position on the facts as 'quibbling' such as that C was at risk prior to D's disclosures or that there is no evidence to show that the admitted disclosures increased the risks to C from other actors, such as Russian intelligence or organised crime. Indeed to the contrary the conclusions of DJ Baraitser, together with the principle that I must take into account not only the evidence actually placed before me on the application for summary judgment, but also the evidence that can reasonably be expected to be available at trial were ample for present purposes.

C's reply to D's application for strike-out

84. Per Peter Gibson LJ in *Hughes & Ors v Richards* [2004] EWCA Civ 266, citing the speech of Lord Browne-Wilkinson in *Barrett v LB Enfield* [2001] 2 AC 550 at 557: "*The correct approach is not in doubt: the court must be certain that the claim is bound to fail. Unless it is certain, the case is inappropriate for striking out*" (cf also *Oysterware Ltd v Intentor Ltd & Ors* [2018] EWHC 611 at para 40 per Joanna Smith QC sitting as a Deputy High Court Judge, describing the power under CPR 3.4(2)(a) as "*only a remedy to which the court should resort in plain and obvious cases*". C

[12] Quoted from C's skeleton.

submitted (uncontroversially) that it is also not appropriate to strike out in areas of the law which are "*uncertain and developing*" (Lord Browne-Wilkinson in *Barrett* at 577; and *Vedanta Resources PLC & Another v Lungowe & Others* [2019] UKSC 20 per Lord Briggs at para 48). C argued that that the law in relation to the LED and Part 3 of the DPA in the context in this case is one such area.

85. As to D's position that it was obliged by paragraph 2.12.2 of the SIRENE Manual and Art 8(1) of the SIS II Decision to disclose alias information to the Latvian authorities and, consequently, that it was "necessary" for D to do so for the law enforcement purposes under the LED C's position was that para 2.12.2 of the Manual was directed at the need "*to avoid incompatible alerts of any category due to an alias to be entered, to avoid problems for innocent victims and to ensure sufficient data quality*". It was there to ensure that persons did not escape detection in cases of mistaken identity (hence I infer its significance where a country making a request provides alias information to the arresting country).

86. On the facts said C, no such risk of confusion with a different suspect arose in C's case: the UK authorities had already dealt with one request for his extradition without needing to disclose his British identity to the Latvian authorities. The requirement under para 2.12.2 of the SIRENE Manual was not absolute in any case. The obligation was caveated with the expression "*as far as possible*" and had to be read as subject to the requirements of article 4(1)(c) and (f) LED that personal data must be "*adequate, relevant and not excessive in relation to the purposes for which they are processed"* and processed in a manner which *"ensures appropriate security for the personal data*".

87. D's submission actually, it was argued, had the effect that if D was correct that it was obliged to disclose alias information ('come what may' in effect) a member state had to provide alias information even if it was unreliable, irrelevant or excessive or would not be held securely. Thus paragraph 2.12.2 of the SIRENE Manual permits D a measure of discretion as to when to disclose details of a suspect's aliases in order to comply with their right to protection of their personal data under article 8 of the Charter, or it is an inflexible device that requires law enforcement bodies to provide alias data no matter how unreliable, irrelevant or

unsafe. The latter interpretation, said to be D's interpretation, was unsupported by authority and contrary to good sense.

88. The sensitivity of C's British identity and address was obvious enough to any reasonable person familiar with the facts of C's case, as it was to Kent Police and HM Court Service. D relied on Recital 16 to the SIS II Decision that "*the whereabouts [of a suspect] should always be communicated to the issuing judicial authority*" but that recital related to persons against whom an arrest warrant had yet to be issued, to help the issuing judicial authority to "*… decide [whether] to transmit a European Arrest Warrant to the competent judicial authority in accordance with the provisions of the Framework Decision 2002/584/JHA*". It was not a provision which requires the disclosure of suspect's home address as an inflexible rule.

89. It was noted also that the substantive obligation which D relied on was paragraph 2.3(b) of the SIRENE Manual which does not require address data to be provided as such, but only states that form G "*shall provide as much information as possible on the hit, including the action taken in the field*". One notes however that providing the address was 'possible' and indeed was done: C complains however that it was not relevant to either the fact of C's arrest or the processing of the second EAW especially given the sensitivities in play. Nor had its disclosure been considered necessary by D when executing C's arrest pursuant to the 2007 EAW. Accordingly it was arguable that the disclosure was excessive and, therefore, contrary to the requirements of art 4 LED and s37 DPA, cutting across the Framework Decision.

90. In relation to C's claim for misuse of his private information, the same points were made. D's argument was that its countervailing interest was its "*need to comply with its legal obligations*" but on C's case D was required by the provisions of the DPA 2018 and the LED to process C's personal data in a manner that was not excessive or unsafe, yet failed to do so. It was possible to process extradition requests and EAWs without placing him at greater risk from Latvian and Russian elements intent on harming him, as was shown by the processing of the first request without such disclosure.

91. Following the 2002 Framework Decision on the European Arrest Warrant, the EU introduced Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, making clear the requirements to respect data protection rights even in the context of law enforcement processing. The 2008 Framework Decision was, in turn, repealed and replaced by the LED. D could point to no authority that the Framework legislation took precedence over the operation of EU data protection legislation.

92. The SIRENE Manual could not reasonably be said to limit the wider fundamental rights of data subjects under EU Data Protection law and the Charter or ECHR. In the context of this case the necessity to consider the security of C's personal data in the hands of the Latvian SIRENE Bureau, consistent with wider EU and Charter rights was a matter for expert evidence in relation to Latvia but even absent that, it was not a surprising ('unheralded') argument for C to suggest that EU Member States may in some circumstances such as asylum reception conditions or prison conditions be obliged to protect fundamental rights by departing from mutual recognition provisions in other contexts (such as asylum). Here the Home Office had concluded in 2001 that C faced a real risk of ill-treatment contrary to article 3 ECHR if returned and DJ Baraitser made the findings cited above as to C's position in risk terms if returned.

93. Accordingly C argued that his statement of case discloses ample reasonable grounds for bringing his claim.

C's reply to D's application for summary judgment

94. There was a "realistic" as opposed to a "fanciful" prospect of success: *Swain v Hillman* [2001] 1 All ER 91 at page 92(j). A "realistic" claim is one that carries some degree of conviction. This means a claim that is more than merely arguable: *ED & F Man Liquid Products v Patel* [2003] EWCA Civ 472 at para 8. Cf also *Easyair Ltd v Opal Telecom Ltd* [2009] EWHC 339 (Ch) at para 15.

95. For the same reasons as set out above, there was a realistic prospect of success.

Part IV: D's response to C

Relationship of the of the Framework Decision, SIS II Decision and SIRENE Manual to the LED and Pt.3 DPA 2018

96. I have framed the points here as D's response to C, though some points were made at the outset of the hearing. For ease of exposition I have placed them here in the narrative. D said that C was incorrect to suggest that it was wrongly giving primacy to the Framework Decision, SIS II Decision and SIRENE Manual.

97. The Framework Decision at Recital 14 referred to the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The first EU instrument properly so called which specifically adopted provisions in relation to the processing of personal data in respect of criminal and justice matters was Council Framework Decision 2008/977/JHA of 27 November 2008 which was repealed and replaced by the LED. The position under the LED was in Art.60 as follows**:**

> *"**Union legal acts already in force***
> *The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, **shall remain unaffected.**"*

98. The SIS II Decision was it was said such a specific provision that was already in force. The SIRENE Decision and the SIRENE Manual were adopted under that Decision. Recital 25 of LED also specifically provided that the LED "*should be without prejudice to the specific rules laid down*" in the SIS II Decision. Art.60, and Recital 94 were also cited in support of the same point as was Recital 39 of the predecessor to the LED, the 2008 Framework Decision. These are discussed in more detail in Part V (decision and reasons).

99. Art.1(2)(b) LED provided that:

"In accordance with this Directive, Member States shall:

...

... ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

100. Secondly, C was incorrect to suggest that D was relying only on the SIRENE Manual. The SIS II legal instruments (the SIS II Decision, the SIRENE Decision and the SIRENE Manual) had to be read together (cf Recital 4 of the SIS II Decision).

101. Thirdly, C's reading of the provisions that they are all subject to the LED made no sense: the SIS II Decision sets out a regime dealing with the protection of data being transmitted pursuant to it such as by providing for the types of data that may be processed (Art.20), who can have access (Arts.40-43), data retention (Arts.44-45), general rules on data processing (Arts.46-55), data protection (Arts.56-63), and penalties (Arts.64-65). This was then elaborated upon in respect of supplementary information in the SIRENE Manual. D's understanding that the EU instruments in play here set out a specific and bespoke set of rules governing the kind of processing that it was engaged in was correct and to the effect that where SIRENE Bureau processed data in compliance with the rules set out in those provisions, it was simply misconceived to seek to ask a further question as to whether the processing also complies with the general obligations under the LED such as 'necessity' for the reason that the SIS II Decision, SIRENE Decision and SIRENE Manual specify what is lawful, fair, necessary, or adequate.

102. As to the meaning of 'necessity' in any event, D, argued that it meant 'reasonably necessary' and sought to distinguish C's authorities as being not on point. *Elgizouli* referred to 'necessity' under s.73(2) of the DPA but that is a provision limited to "Third Country" transfers, ie to non-EU countries. Lord Carnwath's decision was said to represent the majority view in that case as to necessity being a strict test, but in that context, and it appears the point went by agreement. The Court referred to *Guriev*, which related to exemptions under the DPA 1998 *not* the DPA

2018, and being about exemptions (ie that they should be read 'strictly') which was a different point than the one in this case.

103. The decision of Knowles J in *Driver* cited by C was about disclosure by the CPS and was in relation to s.35(2)(b) of the DPA 2018, and the test of 'necessity' there. *Elgizouli* and *Guriev* were referred to but it appeared that the court was unaware of the facts that the former related to Third Country data transfers and the latter related to DPA 1998 exemptions and not 'necessity' in the context of the DPPs.

104. *Cooper* concerned a County Court Data Protection claim about information provided to NCA by Sussex Police and an appeal from the EAT on an employment dispute against the NCA. An issue on the appeal to the Court of Appeal was that the county court had taken too lax a view of the meaning of the word 'necessary' in the data protection claim and that the correct meaning should be a strict one and not 'reasonably necessary'. That decision on appeal, and the authorities relied on in the first instance decision were reviewed by the court and found to be correct. The test, per that authority, was one of reasonable, and not strict necessity accordingly.

Interpretation of the SIRENE Manual provisions

105. Paragraph 2.12.2 of the SIRENE Handbook was not, per contra to C's argument limited to ensuring persons did not escape detection in cases of mistaken identity. The reasons for entering aliases included for example "*to ensure sufficient data quality*". It was very clear as to the scope of the obligation: "*Member States shall as far as possible inform each other about aliases"*.

106. C's interpretation also ignored references to entering aliases in subsequent sections of the Manual and was inconsistent with the fact that alias information was required information (where available to an issuing authority) when completing an EAW.

107. The SIRENE Manual used the expression "*as far as possible*" which plainly did not give rise to a need for a discretionary assessment before disclosure – it amounted to a practical implementation of the notion of all relevant information, ie excluding cases where information was not available or was *de minimis*.

108. The point was made that C had not been detained at the time of the Alias Disclosure (and was not actually arrested until some months later), and hence Alias information was potentially necessary if he had, for example, left for another member state by that point using that alias: so even if contrary to D's position some additional assessment of 'necessity' was required, the alias disclosure would have passed such an assessment.

109. Leaving aside the 'alias' point above, in any case C had lawfully changed his name and his new name was not in reality even an alias. As to address, the form G and Annex to the Framework Decision required residence or address to be treated as potential identifying information.

Reliance on the EU Charter

110. Articles 7 and 8 of the EU Charter are subject to limitations which meet objectives of general interest recognized by the Union (see Art. 52(1) of the Charter). Hence the SIS II Decision and SIRENE Manual set out just such limitations in pursuit of the objective of efficient communication between judicial authorities of Member States. Moreover the SIS II Decision was enacted respecting Charter Rights (see Recital 35). It contained what the EU legislative organs considered to be a proportionate and necessary set of limitations on the rights set out in Arts. 7 and 8. Neither the SIS II Decision nor the SIRENE Manual contained any indication that there should be an individual risk assessment or Charter rights assessment before disclosures of information were made to other Member States' SIRENE bureaux.

111. The point was made that if such assessments were required they would cut against the principle of mutual recognition.

Alleged risk of harm to the Claimant

112. The original alleged offences with which C was charged, the first extradition proceedings, the grant of Exceptional Leave to Remain by the Secretary of State for the Home Department all date from the late 1990s and early 2000s. This was before Latvia acceded to the EU in 2004 and D could not be expected given that change of situation, to have known that the allegations underpinning the 2007 EAW and 2019 EAW would be found to be false until the Westminster Magistrates

Court so found in September 2020. To suggest that D was required to make such an assessment before disclosure would be contrary to the whole EAW and SIS II regimes which at the time of the 2007 and 2019 EAWs were in place between EU member states, by then including Latvia.

113. The fact that the list of alleged threats listed at Particulars of Claim para. 29, included a number dating from before the disclosures, undermined the inference that he invited the Court to make that the threats were from Russia and made use of information supplied to Russia via the Latvian Bureau as a result of the Alias and Address Disclosures (I infer that insofar as this is relevant to a summary judgment if at all, it is a point going to likelihood of success on the facts).

114. The fact that D questioned Latvia's request for C's home address on 23 July 2018 does not assist, in D's view, because at that stage D had no obligation to provide it and came under such an obligation only later when he was arrested, triggering the need for a form G. Likewise the fact that such information was not provided after the October 2018 arrest is of no relevance since C was discharged before appearing before a magistrate because of delay and the case did not reach the stage where a form G was required.

115. The 1999 extradition request was executed without C's UK identity but Latvia was not a Member State of the EU at the time and in any case the EAW regime had not yet been introduced even in the EU.

116. Evidentially C's case also faced admissibility issues: on the question whether any disclosures increased the risk to which C was exposed, the District Judge in the extradition proceedings was not seized of the issue of whether C would be at risk in the UK – she was solely concerned with addressing whether extradition was barred under s.13 of the Extradition Act 2003; and even if C sought to rely on the District Judge's findings as evidence in this Court at an eventual trial (as evidence I could reasonably expect to be before the court at that stage), such would be, it was said, inadmissible. D was not a party to the extradition proceedings and any judgment in such proceedings being *in personam*, rather than *in rem*, would be inadmissible (*Rogers v Hoyle* [2014] EWCA Civ 257, [2015] QB 265, per

Christopher Clarke LJ at [33]-[40] applying the rule in *Hollington v F Hewthorn & Co* [1943] KB 587; cf. Phipson on Evidence (20th ed., 2021) at para. 43.79).

Part V – Decision and reasons

European Arrest Warrants: the intention

117. The starting point in this case is 2002/584/JHA Council Framework Decision of 13 June 2002 which has been referred to throughout as 'the Framework Decision', not to be confused with other similarly named instruments. It created the European Arrest Warrant.

118. Its purposes and policy context can be divined from its Recitals. We see for example the statements that:

"Traditional cooperation relations which have prevailed up till now between Member States should be replaced by a system of free movement of judicial decisions in criminal matters…" (Recital 5) and that:

"The European arrest warrant … is the first concrete measure in the field of criminal law implementing the principle of mutual recognition which the European Council referred to as the 'cornerstone' of judicial cooperation." It is *"based on a high level of confidence between Member States"* (Recital 10).

119. The EAW is thus regarded by the EU as central to a greater degree of cooperation between states which goes beyond the hitherto normal provisions of extradition by states and extends to a more nearly 'administrative' process of 'surrender' of a person subject to an EAW.

120. Recital 5 states expressly the key change namely that of "*abolishing extradition between Member States and replacing it by a system of surrender between judicial authorities".* Within that expression we see not only the shift from extradition to surrender but a shift between 'Member States' in their Sovereign sense to, instead, the role of Judicial Authorities within states. That the creation of this new system was quite radical appears from the following statement in Recital 9: *"The role of central authorities in the execution of a European arrest warrant must be limited to practical and administrative assistance."*

121. Set against this, there is appreciation in the Framework Decision itself that the fundamental rights of suspects still have to be protected. We see from Recital 12 that the Framework decision in *"respects fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union".* We see, in the Charter, rights which are virtually identical to those in the ECHR such as freedom from torture or inhuman and degrading treatment as well as privacy rights. One can conclude therefore that the intention of the EU is that the Framework Decision should respect fundamental rights in the Charter. One must interpret it consistently with that intention.

Execution of an EAW is envisaged as mandatory

122. Execution is intended to be mandatory: Article 1 states that "*Member States shall execute any European arrest warrant on the basis of the principle of mutual recognition and in accordance with the provisions of this Framework Decision."*

123. Consistent with the above principle that the Framework Decision is intended to operate in accordance with the EU Charter of Fundamental Rights, as mentioned above Article 1 must be understood, in my judgment as '*shall (consistent with the provisions of the Charter of Fundamental Rights of the EU) execute any arrest warrant*'. Arts. 7 and 8 of the Charter relate to data processing and connected privacy rights and incorporate notions of processing based on "fairness*",* "specified purposes*"* and on a *"*lawful basis*"* which must in my judgment therefore be said to apply when executing EAWs, as must other EU Charter Rights.

124. We further see that Recital 14 of the Framework Decision states that "*personal data processed in the context of the implementation of this Framework Decision should be protected in accordance with the principles of the [1981 Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data]*", and that the 1981 Convention requires "*adequacy*", "*relevance*" and "*non-excessiveness*" in relation to the purposes for which they are stored.

125. Thus to the mandatory requirement to execute an EAW one adds the interpretive requirement that data processed in the execution of an EAW must be processed consistently with principles of adequacy, relevance and non-excessiveness.

Content of an EAW

126. Article 8(1)(a) of the Framework Decision specifies what information an EAW shall contain. It includes for example the identity of the 'wanted' person, and the standard form of Warrant to be completed (in this instance by Latvia) includes space for name, forename(s), aliases and residence and/or known address. It is fairly obvious that an Issuing Authority when sending an EAW to an Executing Authority should give information sufficient to enable the correct person to be arrested. However that is clearly a different question from the question of what information an Executing Authority, having executed a Warrant, should or is required to give to the Issuing Authority, where the purposes of providing such information would be different. That the purpose of the provision of information to the Executing Authority in the Warrant is the operational one of ensuring that the correct person is arrested is underscored by para. 3.2.1 of the 'Handbook' for EU members on how to issue and execute a European arrest warrant (2017/C 335/01).

"3.2.1. Information that is always necessary

The executing judicial authority should always have the minimum necessary information to allow it to decide on surrender .... In particular, the executing judicial authority needs to be able to confirm the identity of the person ..."

127. Provided the Executing Authority has enough information to effect the arrest then "*In line with the principle of mutual recognition, the executing judicial authority may not question the merits of decisions by the issuing Member State's judicial authorities.*" (para 4.4.1 of the Handbook quoted above). There are provisions (to be treated as 'exceptional') where an Executing Authority can ask for 'supplementary information'. The Handbook states also at 4.4.1:

"If the information communicated by the issuing Member State is insufficient to allow the executing judicial authority to decide on surrender, the executing judicial authority has a duty[13] to communicate with the issuing judicial authority in order to obtain the necessary supplementary information. Communication between the issuing and executing judicial authorities prior to the surrender decision should

[13] Art 15(2) Framework Decision.

primarily concern supplementary information that is relevant for deciding on surrender (see Section 5.6). Thus, requests for supplementary information should concern, in particular, the content required in the EAW form which is needed to assess the possibility to execute the EAW and the applicability of any ground for refusal."

128. We see therefore that where the Framework Decision uses the expression 'supplementary information' it focusses primarily on information necessary to execute the warrant against the correct person.

Implementing the EAW regime practically: the SIS II decision and SIRENE Manual

129. Recital 10 to the SIS II Decision (ie Council Decision 2007/533/JHA of 12 June 2007) states the linkage between information in the SIS II system and the EAW process itself both in terms of 'alerts' and 'supplementary information':

"SIS II is to contain alerts on persons wanted for arrest for surrender purposes and wanted for arrest for extradition purposes. In addition to alerts, it is appropriate to provide for the exchange of supplementary information which is necessary for the surrender and extradition procedures. In particular, data referred to in Article 8 of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States should be processed in SIS II"

The obligation on the Executing Authority to disclose information on a Form G

130. SIRENE Manual para 2.3 provides that:

Unless stated otherwise, the issuing Member State shall be informed of the hit and its outcome ...

The following procedure shall apply:

(a) Without prejudice to Section 2.4 of this Manual, one hit on an individual ... for which an alert has been entered, shall in principle be communicated to the SIRENE Bureau of the issuing Member State using one G form.

(b) ... The G form shall provide as much information as possible on the hit, including on the action taken in field 088. Provision of supplementary information may be requested from the issuing Member State in field 089 ...

131. This is important for D's case: the Manual for the SIRENE system mandates the use of so-called form G (the form on which information was disclosed in this case) and requires the Executing Authority to provide "as much information as possible" on that form.

132. The Framework Decision requires that the principles of the 1981 Convention be applied in relation to EAWs, but we also see that SIS II Decision addresses the 1981 Convention requirement by stating via Recital 19 that the substantive Articles of SIS II are to 'supplement or clarify' those principles' in the 1981 Convention[14]. We see moreover at Recital 34 of the SIS II Decision that "*(34) This Decision* [ie, including any respects in which the Decision clarifies or supplements the 1981 Convention Provisions as expected by Recital 19] *respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union."*

133. C's counsel referred (as an example rather than a binding decision) to Case C-88/21[15] where Lithuania had passed a law preventing any vehicle being registered if there was any alert on SIS II. In the opinion of the Advocate General para. 80 it was stated that "*the fundamental rights enshrined in the Charter are binding on the Member States when acting in the scope of EU law*" and that inter alia the rules laid down in the SIRENE Manual naturally fell within the scope of EU law and had to comply with the fundamental rights enshrined in the Charter. Accordingly in my judgment the Framework Decision and its operational implementation by SIS II, and implicitly the SIRENE manual, are intended to be applied consistently with the 1981 Convention and the EU Charter but the 1981 Convention can be

[14] *"(19) … The Convention allows exceptions and restrictions to the rights and obligations it provides, within certain limits. The personal data processed in the context of the implementation of this Decision should be protected in accordance with the principles of the Convention. The principles set out in the Convention should be supplemented or clarified in this Decision where necessary...."*

[15] Opinion of Advocate General Emiliou in Regionų apygardos administracinio teismo Kauno rūmai, delivered on 7 July 2022.

supplemented or clarified by the SIS II Decision. SIS II is thus not 'neutral' with respect to the 1981 Convention and is an instrument through which that Convention needs to be seen and to which the Charter and Convention have to be applied.

The role of the Law Enforcement Directive and the Data Protection Act 2018

134. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (the LED) post-dates the 1981 Convention, the Framework Decision, SIS II Decision and SIRENE Manual. It is common ground that Part 3 of the Data Protection Act 2018 implements the LED. The LED was described by D's counsel as in effect a 'partner' to the General Data Protection Regulation 2016 ("GDPR") – a regulation which therefore took direct effect - and which came into force in May 2018.

135. Recital 2 of the LED states "*principles of, and rules on the protection of natural persons with regard to the processing of their personal data <u>should, whatever their nationality or residence, respect their fundamental rights and freedoms,</u> in particular their right to the protection of personal data*".

136. At Recital 51 it declares that *"… risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to .... loss of confidentiality of data"*.

137. Article 4(1) provides that personal data must be:

> (a) processed lawfully and fairly; …
> (c) adequate, relevant and not excessive in relation to the purposes for which they are processed; …
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss, destruction or damage, using appropriate technical or organisational measures.

138. The DPPs in the UK's DPA, Part 3 effectively implement Art. 4(1) above.

The interaction or non-interaction between the LED/Data Protection Act 2018 and the Framework Decision/SIS II system: the question of whether there are "carve outs" from the DPA and LED for the EAW and SIS II arrangements.

139. I next consider the predecessor to the LED, namely Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

140. It had recently ceased to be in force at the material time but contained a recital at 39 which foreshadowed material in the later LED and which in D's view confirmed the conception that the special provisions as to law enforcement data sharing were intended to constitute a 'complete code' and not be affected by more general data protection provisions such as those in the 2008 Framework or, later, the LED.

141. That Recital stated among other things:

"Several acts, adopted on the basis of Title VI of the Treaty on European Union, contain specific provisions on the protection of personal data exchanged or otherwise processed pursuant to those acts. In some cases these provisions constitute a complete and coherent set of rules ... The relevant set of data protection provisions of those acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision."

142. Turning to the LED which replaced the above 2008 Framework Decision we see that Art.60 of LED states that:

"*… specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.*"

143. We similarly see Recital 94 which is very close to the former Recital 39 in the 2008 Framework Decision: *"Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected … ".*

144. Recital 25 of the LED states that the LED "*should be without prejudice to the specific rules laid down*" in the SIS II Decision.

145. Furthermore Art. 1(2) of the LED requires that Member States shall:

(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

(b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data;"

How are the above provisions (apparent 'carve outs') to be understood against the backdrop of the Framework Decision and SIS II Decision?

146. LED Art. 1(2)(b) and Art 60 and Recital 94 are especially strongly and clearly worded. They assist D. Their wording meshes with the principle in Recital 25 that the LED is 'without prejudice' to specific rules in the SIS II Decision and it is credible to say that they have their origins in the (repealed) provisions of Recital 39 of the above-quoted 2008 Framework Decision as the predecessor of the LED.

147. In my judgment these LED provisions therefore mean that *provided that an exchange of data between competent EU authorities is required by EU or Member State law* (per LED Art 1(2)(b)) then the LED and legislation implementing it must not be applied so as to restrict or prohibit that transfer.

148. I agree therefore that SIS II and the Framework Decision are a specific code devoted to the special case of the EAW Regime and its policy objectives which were discussed above and it is clear in my judgment that the intention is that they have a special status protected by the express restrictions within the LED upon what might be called 'interference' with the EAW regime data sharing system. To that extent I agree with D that LED or DPA provisions ordinarily cannot 'restrict or prohibit' the Framework Decision's effects requiring data sharing, and a compliance with the Framework Decision and SIS II would suffice to permit transfer. The 'special' nature of the EAW system would prevail, without debate over the protection of the individual data subject's rights in DPA or LED terms.

149. Section 80 of the DPA appears to me to be giving effect in UK law to Art 1(2)(b) of the LED which bars any restriction or prohibition of inter-authority data transfers for law enforcement where required by an existing law.

As far as material it states:

> "*80. (3) The controller must consider whether, if the personal data had instead been transmitted or otherwise made available within the United Kingdom to another competent authority, processing of the data by the other competent authority would have been subject to any restrictions by virtue of any enactment or rule of law*[16]*.*
>
> *(4) Where that would be the case, the controller must inform the EU recipient … that the data is transmitted or otherwise made available subject to compliance by that person with the same restrictions (which must be set out in the information given to that person).*
>
> *(5) Except as provided by subsection (4), the controller may not impose restrictions on the processing of personal data transmitted or otherwise made available by the controller to an EU recipient.*"

[16] Such as, say, the DPA 2018.

150. It seems therefore clear that where a Controller is required by law (EU or member state) to transfer data pursuant to the pre-existing SIS II and EAW regimes, the Controller is obliged to do so, normally, and the limit of the 'restriction' which may be imposed is that stated in s.80(4) and (5) namely the informing of the EU Issuing Authority, as recipient, that the disclosure is made subject to compliance with relevant law. Notably subsection (5) expressly bars the imposition of any other restriction (which would in my judgment include a refusal to provide the data).

The role of fundamental rights?

151. The above begs the question though as to when exchange of data between competent authorities is "required" by EU or Member State law. If it is required then it falls within LED Art 1(2)(b)'s limitation on the restriction or prohibition of data sharing which underpins the 'carve outs' referred to above and also in my judgment underpins s.80 of the DPA. It does not, however, resolve the case of a proposed exchange of information between Competent Authorities where for example countervailing principles of ECHR human rights law or EU Fundamental Charter law, or indeed simply the wording of LED Art 1(2)(a) itself (requiring as it does the protection of fundamental rights) or Art 1(3) of the Framework Decision referring to fundamental rights, apply to the effect that a particular transfer of information would be contrary to fundamental rights.

152. In my judgment disclosure, if it would be contrary to fundamental rights, would not be strictly 'required' (per Art 1(2)(b) LED) by EU or Member State Law so as to engage the 'carve outs'. The Executing Authority would then arguably be obliged to apply the DPA's Data Protection Principles, and could impose restrictions or refuse the transfer either outright or unless modified to protect fundamental rights. One could not simply say it had automatically met all required legal criteria such as 'necessity' by following the EAW and SIS II processes, if a breach of fundamental rights would mean that transmission was not lawfully required.

153. Dealing with the impact of fundamental rights, D argued that the role of the EU Charter of Fundamental Rights was mitigated by Art 52 thereof allowing

limitations on Charter Fundamental Rights and was mitigated by Art 52 thereof allowing limitations on Fundamental Charter Rights and which as far as material says: *"limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."*

154. Hence the point was made by D that SIS II and the Framework Decision were just such 'limitations'. It does not seem to me that they contain provisions which effectively oust or limit protections under the EU Charter and 1981 Convention to such extent that competent authorities do not have a discretion to exercise where there would be an arguable breach of fundamental rights in the event of disclosure. There is much in all of the instruments cited in this judgment which to the contrary stresses the legislative intention that fundamental rights are not overridden.

155. Thus in my judgment in considering the making of a disclosure in the circumstances of this case it is arguable that D should have considered whether doing so was truly 'required' by the Framework Decision/SIS II once one took into account ECHR and EU Charter provisions in interpreting and applying the Framework Decision, given the factual background specific to this case. What it should have done after considering that is a matter for trial.

156. It cannot therefore be said with sufficient certainty in my judgment that C's case on the application of the Framework Decision and SIS II in relation to the DPA and LED is fanciful or lacks a proper basis for argument in law.

Was disclosure <u>unarguably</u> lawful under the EAW and SIS II provisions read with the SIRENE Manual?

157. At risk of effective repetition, it is plainly arguable that the purpose of the Framework Decision and the SIS II Decision is to give effect to the very high degree of administrative implementation expected from the EAW system. I noted for example the shift, in the EAW Framework Decision, away from extradition and cooperation between EU states and towards 'surrender' of suspects and the execution of warrants. It is arguable therefore that the effect of the EAW

Framework Decision and SIS II provisions is a rebalancing of data subjects' rights in favour of the UK State's duty to execute Warrants. I reviewed immediately above for example the quite strong indications to that effect notably in Art 1(2) of the SIS II Decision among other provisions.

158. However it will be clear from my comments above that I cannot go as far as holding that the wording of the SIS II Decision or the Framework Decision is so plain that the 'clarification' or 'supplementation' which it provides to EU data protection law, and the possible 'carve outs' such as that in Art 1(2)(b) of SIS II, are such as to deprive data subjects of any degree of discretion inherent in the Executing Authority where fundamental rights are concerned, and it was noted above that the Framework Decision expressly refers in its Recitals to the fact that the EU Charter and 1981 Convention apply to it (Recitals 12 and 14).

159. The concept that certain sorts of data must be provided in form G and that '<u>as much information as possible</u>' "<u>must</u>" be provided when the Executing Authority reports back, does not in my judgment amount to a sufficiently clear statement that EU Charter provisions, 1981 Convention provisions, or the ECHR are rendered effectively irrelevant when an Executing Authority is charged with carrying out the EAW process's data transfer provisions. "As much information as possible" should arguably mean "reasonably and lawfully possible" unless the highly improbable meaning is to be inferred that even the most trivial or inaccurate or risk laden information must be supplied come what may. One would expect the clearest of derogations to be included if the EU Charter, for example, was to have no role in the decision as to providing information on form G.

"necessity"

160. The case law on the question whether 'necessity' within the DPPs means '*strictly necessary*' or '*reasonably necessary',* which was a point of difference between the parties does not appear to me to demand a ruling given my decision above.

161. I do not need to rule on the point because, whatever the test, if on a trial on evidence there was no question of a breach of fundamental rights through making disclosures under the EAW system it seems to me that the 'carve outs' in

the LED prevent the DPA from restricting or prohibiting transfer irrespective of how one approaches 'necessity' in DPP terms. Conversely the question of necessity is a fact specific one not amenable to summary disposal if, as I find to be arguable, the DPPs *do* apply where there is (as there arguably is) a breach of fundamental rights in the event of disclosure being made such that the carve-outs in favour of the EAW process in the LED no longer applied on the facts of this case.

The evidence (or lack of it) of Alleged risk of harm to the Claimant caused by the Disclosures

162. In my judgment the material set out in the pleadings and evidence suffices to set out a case which is not inherently contradictory or implausible as to whether disclosure to the Latvian Authorities might place C at risk as a matter of fact. I need not resolve the issue raised by D over the strict admissibility of the decision of DJ Baraitser and evidence at that extradition hearing, but in considering the case in the round I have to consider what evidence it is reasonable to anticipate would be before the court at trial in this action, and it is not fanciful to suppose that C could marshal evidence going to the issues which were canvassed before DJ Baraitser and which inter alia pointed to C being at risk of serious harm from both Russian and Latvian actors. Establishing by evidence a link between risk of that sort, and the possible role of disclosure of personal data in leading to or worsening risk, and the potential for liability of D given what it did know about C's status at the time of the disclosures[17] is not something lacking in real prospect of success at a trial on evidence.

Common law claim: misuse of private information (MPI).

163. As to the common law in relation to the tort of misuse of private information, it is not in dispute that there is a two-stage test for the tort of MPI, namely: (1) whether the claimant's right to privacy under Art.8 ECHR was engaged by the

[17] D did not of course have the evidence later produced to the District Judge, but it appears D was aware of the previous refusal of extradition and reasons for it. It is not fanciful that a case could be made out that D knew or ought to have known of a probable increase in risk to C if it disclosed information.

defendant's use of the information such that they had a reasonable expectation of privacy; and (2) whether the claimant's reasonable expectation of privacy was outweighed by countervailing interests (*McKennitt v Ash* [2006] EWCA Civ 1714, [2008] QB 73, per Buxton LJ at [11]). For the purposes of the present Application it is uncontroversial that the first limb of the above is assumed to be satisfied.

164. In my judgment I need say no more than what has been said above in relation to the EU provisions and DPA to deal with the claim in relation to common law Misuse of Private Information which is a species of Member State law in this instance. If the EU Law provisions did require disclosure in this case notwithstanding factors considered under the ECHR or the EU Charter, then it is probable that the 'reasonable expectation of privacy' would be outweighed by the countervailing interest of the State in giving effect to the provisions of the EAW. On the other hand if, properly applied D ought to have considered the impact of considerations such as Art 3 risks of disclosure or risks of breach of the EU Charter and concluded that disclosure was a disproportionate interference, then it is not fanciful to suppose that common law claim for MPI would lie given the evidence which it is reasonable to anticipate would be available at trial.

165. It follows from the above that I dismiss the application.

IN DRAFT to parties 27 July 2023

HANDED DOWN 27 October 2023

JUDGE: MASTER VICTORIA MCCLOUD

Annex – legal provisions

Data protection in the context of Law Enforcement in criminal matters

1. The 2008 Framework Decision ("Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters") was the first effort of the EU to create a set of rules governing data processing in the context of criminal judicial cooperation within Europe. It was repealed shortly before the disclosures in this case but it sets the background to the provisions which replaced it namely the GDPR and most importantly in this context the Law Enforcement Directive (LED). The parties referred to various provisions as part of charting the course of how the LED came to have its present form.
2. Recital (4) referred to "*the need for an innovative approach to the cross- border exchange of law-enforcement information under the strict observation of key conditions in the area of data protection*"
3. Recital (5) stressed the need for "*clear rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in respect of such cooperation between the Member States while fully respecting fundamental rights of individuals*". It went on to note that "*[e]xisting instruments at the European level do not suffice*";
4. Recital (39) stated "*Several acts, adopted on the basis of Title VI of the Treaty on European Union, contain specific provisions on the protection of personal data exchanged or otherwise processed pursuant to those acts. In some cases these provisions constitute a complete and coherent set of rules covering all relevant aspects of data protection (principles of data quality, rules on data security, regulation of the rights and safeguards of data subjects, organisation of supervision and liability) and they regulate these matters in more detail than this Framework Decision. <u>The relevant set of data protection provisions of those acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing</u>*

direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision. …

5. Recital (40) stated that, in relation to the 1981 Convention, where provisions of EU or national legislation imposed, in other cases than those in recital (39) where, "*conditions on receiving Member States as to the use or further transfer of personal data are more restrictive than those contained in the corresponding provisions of this Framework Decision, the former provisions should remain unaffected. However, for all other aspects the rules set out in this Framework Decision should be applied*";
6. Article 1(2) required Member States to "*protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy*" when sharing data for law enforcement purposes;
7. Article 3(1) provided that "*[p]rocessing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected*"

The Law Enforcement Directive (LED)

8. The Law Enforcement Directive[18] replaced the 2008 Framework Decision referred to above. At the time of the processing of personal data and the admitted disclosures, the UK was an EU member and was subject to the LED.

   Recital (1) provides that the "*protection of natural persons in relation to the processing of personal data is a fundamental right*";

   Recital (2) states that the "*principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data*";

[18] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data, referred to as the Law Enforcement Directive.

Recital (25) states that "*Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in [the SIS II Decision].*"

Recital (46) provides that *"[a]ny restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms*";

Recital (51) provides a statement that "*… risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to .... loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation*";

Recital (94) states: "*Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected …*"

9. Art.1(2)(b) of the LED provided that:

"In accordance with this Directive, Member States shall:

...

... ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

10. Article 4(1) provides that personal data must be:

(a) processed lawfully and fairly; …

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed; …

(f) processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss, destruction or damage, using appropriate technical or organisational measures.

11. Article 60 states:

"**Union legal acts already in force**

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected."

The Data Protection Act 2018

12. Part 3 of the DPA 2018 implements the LED in the UK. The Directive came into force in May 2018. The date of data processing in this case was before the UKs exit from the EU in 2020 and before the end of the 'Implementation Period' for Brexit which ended at the end of 2020.
13. The Director General of D is referred to as a "*competent authority*" under s.30(1)(a) DPA 2018 (and Sch.7 DPA 2018). The Disclosures to the Latvian Bureau were therefore done by a 'competent authority' and so were processing to which Pt.3 DPA 2018 applies. Section 31 DPA 2018 defines "*law enforcement purposes*" as, *inter alia*, "*... the purposes of the ... investigation ... or prosecution of criminal offences ...*".

14. Sections 35-40 of Part 3 of the Act provide six Data Protection Principles ("DPPs") governing the processing of personal data by a controller for law enforcement purposes. I shall quote the ones in play in this case which are DPPs 1, 3 and 6.

15. Section 35 DPA 2018 provides (in part):

*"**35 The first data protection principle***

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and ...—

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority."

16. Section 37 provides:

*"**37 The third data protection principle***

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."

17. Section 40 provides:

*"**40 The sixth data protection principle***

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)."

The Data Protection Act 2018 on the subject of law enforcement transfers to EU competent authorities

18. Section 80 provides:

80(1) Subsections (3) and (4) apply where, for a law enforcement purpose, a controller transmits or otherwise makes available personal data to an EU recipient or a non-EU recipient.

(2) In this section—

"EU recipient" means—

(a) a recipient in a member State other than the United Kingdom, or

(b) an agency, office or body established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union

(3) The controller must consider whether, if the personal data had instead been transmitted or otherwise made available within the United Kingdom to another competent authority, processing of the data by the other competent authority would have been subject to any restrictions by virtue of any enactment or rule of law.

(4) Where that would be the case, the controller must inform the EU recipient … that the data is transmitted or otherwise made available subject to compliance by that person with the same restrictions (which must be set out in the information given to that person).

(5) Except as provided by subsection (4), the controller may not impose restrictions on the processing of personal data transmitted or otherwise made available by the controller to an EU recipient.

European Arrest Warrants ("EAWs") 2002/584/JHA EU Council Framework Decision of 13 June 2002

19. EAWs were established by the EU Council Framework Decision of 13 June 2002[19] on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) ("the Framework Decision" – not to be confused with the repealed 2008 Framework Decision referred to above).

Recital (5) of the Framework Decision states *"The objective set for the Union to become an area of freedom, security and justice leads to abolishing extradition between Member States and replacing it by a system of surrender between judicial authorities. ... Traditional cooperation relations which have prevailed up till now between Member States should be replaced by a system of free movement*

[19] Full title 2002/584/JHA Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States

of judicial decisions in criminal matters, ... within an area of freedom, security and justice.

Recital (6) states *"The European arrest warrant provided for in this Framework Decision is the first concrete measure in the field of criminal law implementing the principle of mutual recognition which the European Council referred to as the 'cornerstone' of judicial cooperation.*

Recital (9) states *"The role of central authorities in the execution of a European arrest warrant must be limited to practical and administrative assistance."*

Recital (10) *"The mechanism of the European arrest warrant is based on a high level of confidence between Member States. Its implementation may be suspended only in the event of a serious and persistent breach by one of the Member States of the principles set out in Article 6(1) of the Treaty on European Union, determined by the Council pursuant to Article 7(1) of the said Treaty with the consequences set out in Article 7(2) thereof.*

Recital (12) states *"This Framework Decision respects fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union, in particular Chapter VI thereof ..."*

Recital (14) requires that "*the personal data processed in the context of the implementation of this Framework Decision should be protected in accordance with the principles of the [1981 Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data]*"

(In turn, Article 5 of the 1981 Convention requires that personal data undergoing automatic processing shall be "adequate, relevant and not excessive in relation to the purposes for which they are stored")

20. The substantive provisions (ie the Articles) of the Framework Decision include the following:

Article 1

Definition of the European arrest warrant and obligation to execute it

…

2. Member States shall execute any European arrest warrant on the basis of the principle of mutual recognition and in accordance with the provisions of this Framework Decision.

3. *This Framework Decision shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.*

Article 6

Determination of the competent judicial authorities

1. The issuing judicial authority shall be the judicial authority of the issuing Member State which is competent to issue a European arrest warrant by virtue of the law of that State.

2. The executing judicial authority shall be the judicial authority of the executing Member State which is competent to execute the European arrest warrant by virtue of the law of that State. ...

Article 7

Recourse to the central authority *.*

2. A Member State may, if it is necessary as a result of the organization of its internal judicial system, make its central authority(ies) responsible for the administrative transmission and reception of European arrest warrants as well as for all other official correspondence relating thereto.

21. Article 8(1)(a) of the Framework Decision specifies what information an EAW shall contain, including the identity of the requested person. The prescribed form of an EAW set out in the Annex to the Framework Decision specifies that the information about the identity of a requested person includes, their name,

forename(s), aliases and residence and/or known address. There exists a 'Handbook' for EU members on how to issue and execute a European arrest warrant (2017/C 335/01) ("the Handbook") which is guidance and is not legally binding.

The EAW Handbook

22. Paragraph 1.2 states: *"The EAW is a judicial decision enforceable in the Union that is issued by a Member State and executed in another Member State on the basis of the principle of mutual recognition.*

...

The Framework Decision on EAW reflects a philosophy of integration in a common judicial area. It is the first legal instrument involving cooperation between the Member States on criminal matters based on the principle of mutual recognition. The issuing Member State's decision must be recognised without further formalities and solely on the basis of judicial criteria."

114. Paragraph 3.2.1 of the Handbook states**:**

3.2.1. Information that is always necessary

The executing judicial authority should always have the minimum necessary information to allow it to decide on surrender .... In particular, the executing judicial authority needs to be able to confirm the identity of the person ..."

115. Paragraph 4.4.1 of the Handbook states that the executing judicial authority may not question the merits of the decisions of the issuing Member State's judicial authorities. By para. 5.1 of the Handbook it is said that:

"*5.1. General duty to execute EAWs*

The executing judicial authority has a general duty to execute any EAW on the basis of the principle of mutual recognition and in accordance with the provisions of the Framework Decision on EAW (Article 1). ..."

The Schengen Information System II (SIS II Decision)

116. To implement the EAW system, information sharing between EU Member States which are members of the second generation Schengen Information System ("SIS II") is governed by the EU Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) ("the SIS II Decision") Latvia and for the purposes of this case, also the UK were part of SIS II.

The recitals to the SIS II Decision provide:

"(6) It is necessary to specify the objectives of SIS II, ... to lay down rules concerning ... the categories of data to be entered into the system, the purposes for which the data are to be entered, the criteria for their entry, the authorities authorised to access the data, ... and further rules on data processing and the protection of personal data.

(8) It is necessary to establish a manual setting out the detailed rules for the exchange of certain supplementary information concerning the action called for by alerts. National authorities in each Member State should ensure the exchange of this information. …

(10) ... In addition to alerts, it is appropriate to provide for the exchange of supplementary information which is necessary for the surrender and extradition procedures. In particular, data referred to in Article 8 of the [EAW] Decision ...

(16) When a flag has been added and the whereabouts of the person wanted for arrest for surrender becomes known, the whereabouts should always be communicated to the issuing judicial authority, which may decide to transmit a European Arrest Warrant to the competent judicial authority in accordance with the provisions of the Framework Decision 2002/584/JHA. ...

(19) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The Convention allows exceptions and restrictions to the rights and obligations it provides, within certain limits. The personal data processed in the context of the implementation of this Decision should be protected in accordance

with the principles of the Convention. The principles set out in the Convention should be supplemented or clarified in this Decision where necessary...

(33) ... In accordance with the principle of proportionality, as set out in Article 5 of the EC Treaty, this Decision does not go beyond what is necessary to achieve those objectives.

(34) This Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. ..."

26. The substantive provisions of the SIS II Decision include:

Article 2

Scope

1. This Decision establishes the conditions and procedures for the entry and processing in SIS II of alerts on persons ..., the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.

Article 3

Definitions

1. For the purposes of this Decision, the following definitions shall apply:

(a) 'alert' means a set of data entered in SIS II allowing the competent authorities to identify a person ... with a view to taking specific action;

(b) 'supplementary information' means information not stored in SIS II, but connected to SIS II alerts, which is to be exchanged supplementary information' means information not stored in SIS II, but connected to SIS II alerts, which is to be exchanged: supplementary information' means information not stored in SIS II, but connected to SIS II alerts, which is to be exchanged:

(i) in order to allow Member States to consult or inform each other when entering an alert;

(ii) following a hit in order to allow the appropriate action to be taken;

(iii) when the required action cannot be taken;

(iv) when dealing with the quality of SIS II data;

(v) when dealing with the compatibility and priority of alerts;

(vi) when dealing with rights of access;

(c) 'additional data' means the data stored in SIS II and connected with SIS II alerts which are to be immediately available to the competent authorities where a person in respect of whom data has been entered in SIS II is located as a result of searches made therein

Article 7

SIS II Office and SIRENE Bureau

2. Each Member State shall designate the authority which shall ensure the exchange of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8.

Those Bureaux shall also coordinate the verification of the quality of the information entered in SIS II. For those purposes they shall have access to data processed in the SIS II.

Article 8

Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual ...

2. Supplementary information shall be used only for the purpose for which it was transmitted.

3. Requests for supplementary information made by other Member States shall be answered as soon as possible.

4. Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 67 in the form of a manual called the 'SIRENE Manual'... ...

Article 20

Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Decision providing for the storage of additional data, SIS II shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Articles 26....

2. The categories of data shall be as follows:

(a) persons in relation to whom an alert has been issued; ...

3. The information on persons in relation to whom an alert has been issued shall be no more than the following:

(a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately; ....

Article 23

Requirement for an alert to be entered

1. Alerts on persons may not be entered without the data referred to in Article 20(3)(a), ...

CHAPTER V

ALERTS IN RESPECT OF PERSONS WANTED FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES

Article 26

Objectives and conditions for issuing alerts

1. Data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant ... shall be entered at the request of the judicial authority of the issuing Member State. ...

Article 40

Authorities having a right to access alerts

2. ... [T]he right to access data entered in SIS II and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.

CHAPTER XI

GENERAL DATA PROCESSING RULES

Article 46

Processing of SIS II data

1. The Member States may process the data referred to in Articles 20, 26... only for the purposes laid down for each category of alert referred to in those Articles.

The SIRENE Decision and SIRENE Manual

27. The relevant edition of the SIRENE Manual ("the SIRENE Manual") is set out in the EU Commission Decision (EU) 2017/1528 of 31 August 2017 ("the SIRENE Decision"). It provides information as to how to operate the SIS II system in respect of supplementary information.

28. Recital (1) to the SIRENE Decision provides:

"*The second generation Schengen Information System (SIS II) ... contains sufficient information allowing the identification of a person ... and the necessary action to be taken. In addition, for SIS II to function effectively, Member States exchange supplementary information related to the alerts. ...*"

29. Paragraphs 1.1, 1.2, 1.15, 2.3 and 2.12 of the SIRENE Manual state:

1.1 The SIRENE Bureau

SIS II only contains the indispensable information (i.e. alert data) allowing the

identification of a person ... and the necessary action to be taken. In addition, according to the SIS II legal instruments, Member States shall exchange supplementary information related to the alert which is required for implementing certain provisions foreseen under the SIS II legal instruments, and for SIS II to function properly, either on a bilateral or multilateral basis.

A national 'SIRENE Bureau' ... shall serve as a single contact point for the Member States ... for the purpose of exchanging supplementary information in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons ... have been entered in SIS II and are found as a result of a hit.

The SIRENE Bureaux's main tasks include ensuring the exchange of all supplementary information is in accordance with the requirements of this SIRENE Manual, as provided in common Article 8 of the SIS II legal instruments for the following purposes:

(a) to allow Member States to consult or inform each other whilst entering an alert (e.g. when entering alerts for arrest);

(b) following a hit to allow the appropriate action to be taken (e.g. matching an alert); …

1.2. SIRENE Manual

The SIRENE Manual is a set of instructions which describes in detail the rules and procedures governing the bilateral or multilateral exchange of supplementary information. …

1.15 Data quality

… In order for the data in SIS II to be kept up-to-date ... the SIRENE Bureau shall take the necessary measures to ensure the prompt updating of alphanumeric data in alerts; either by the SIRENE Bureau itself or by liaising with the relevant

authority which created the alert. This shall cover activities such as inclusion of aliases or correction of identity details …

2.3 The exchange of information after a hit

Unless stated otherwise, the issuing Member State shall be informed of the hit and its outcome ...

The following procedure shall apply:

(a) Without prejudice to Section 2.4 of this Manual, one hit on an individual ... for which an alert has been entered, shall in principle be communicated to the SIRENE Bureau of the issuing Member State using one G form.

(b) ... The G form shall provide as much information as possible on the hit, including on the action taken in field 088. Provision of supplementary information may be requested from the issuing Member State in field 089 ...

2.12 Different categories of identity

Alias

Alias means an assumed identity used by a person known under other identities. …

2.12.2. Entering an alias

... Member States shall as far as possible inform each other about aliases and exchange all relevant information about the real identity of the sought subject. ... If another Member State discovers an alias, it shall inform the issuing Member State using an L form. ...”

The EU Charter of Fundamental Rights

30. Art 52 provides that:

“1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised

by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."