

Memorandum

TO	Standard Chartered Bank	DATE	26 October 2021
COPY TO		FILE REF	70-41021850
FROM	Simon Persoff / Richard Jones	DIRECT DIAL	+44 20 7006 3060 / 8238

Opinion - SEC access to SCB records under English law

1. INTRODUCTION AND BACKGROUND

1.1 We understand that:

- 1.1.1 Standard Chartered Bank ("**SCB**") proposes to register with the U.S. Securities and Exchange Commission (the "**SEC**") as a "nonresident" security-based swap dealer;
- 1.1.2 in connection with this registration, SCB is required¹ to certify that it can, as a matter of law, and will, provide the SEC with prompt access to its books and records and submit to onsite inspection and examination by the SEC (the "**Required Access Arrangements**");
- 1.1.3 SCB is also required² to provide an opinion of counsel with regard to these certifications with respect to laws of the jurisdictions in which SCB maintains such of its books and records as are covered by the relevant U.S. regime ("**Covered Records**")³; and
- 1.1.4 SCB maintains some or all of the Covered Records in England.

¹ Pursuant to 17 CFR § 240.15Fb2-4(c)(1)(i).

² Pursuant to 17 CFR § 240.15Fb2-4(c)(1)(ii).

³ We assume for the purposes of this memorandum that the scope of the books and records that may be accessed by or otherwise disclosed to the SEC will be limited to books and records that are subject to the SEC's jurisdiction under U.S. law and regulation, as indicated in the guidance dated 3 May 2021 provided by SCB's U.S. counsel, Cleary Gottlieb Steen & Hamilton LLP, entitled "*Guidance Re: Opinion of Counsel Requirement for Nonresident Security-Based Swap Dealers*", a copy of which has been provided to us. The term "**Covered Records**", when used in this memorandum, should be interpreted accordingly.

- 1.2 SCB has asked us to provide the required opinion in respect of England. This memorandum does not advise or express an opinion on the laws of any jurisdiction other than England.⁴
- 1.3 We have assumed for the purposes of this memorandum that SCB has not made, and will not make, *express contractual commitments* that are inconsistent with the Required Access Arrangements.
- 1.4 For the purposes of this memorandum we have taken account of the letter dated 11 September 2020 from James Dipple-Johnstone (Deputy Commissioner and Chief Regulatory Officer) of the UK Information Commissioner's Office (the "ICO") to Raquel Fox (at the time, Director of the Office of International Affairs) of the SEC in relation to certain issues arising under UK⁵ data protection law (the "ICO Letter").⁶ The ICO Letter expresses the ICO's views, as of its date, in relation to cooperation by persons subject to UK data protection laws in the Required Access Arrangements.⁷ Although it does not address all relevant issues, and does not bind the ICO as to its future interpretation of UK data protection law, the ICO Letter does provide very substantial comfort as to any likely risk that the ICO, which is the supervisory authority responsible for enforcement of UK data protection law, might take an adverse view where SCB cooperates in the Required Access Arrangements. In particular, the ICO Letter takes the view that UK regulated firms are able to transfer personal data to the SEC in the context of the Required Access Requirements without breach of UK data protection law's restrictions on the international transfer of personal data, on the basis

⁴ Please note that, in some places, we refer to the UK, or UK law, because the laws under consideration form part of United Kingdom law applicable in England rather than specifically English law. In each case, however, we have only considered those laws as they form part of English law and not as they form part of the laws of any other part of the United Kingdom.

⁵ Please note that the ICO Letter was written during the Brexit transitional period following the United Kingdom's exit from the European Union ("EU"), when EU data protection law continued to form part of UK law pursuant to transitional arrangements between the EU and the UK. For relevant purposes, however, it is in our opinion equally applicable to UK data protection law as it stands as of the date of this letter, which is closely based on EU data protection law as at the end of the transitional period. (One difference is that the letter refers to the ICO's obligation to interpret the GDPR (before it was implemented as the UK GDPR) in accordance with the EU Charter of Fundamental Rights. This is no longer the case, but the ICO will be obliged to interpret the UK GDPR in accordance with the UK Human Rights Act 1998 and the interpretative effect of this obligation will in our view be essentially the same for relevant purposes.)

⁶ A copy of the ICO Letter is available on the Internet at <https://ico.org.uk/media/for-organisations/documents/2619110/sec-letter-20200911.pdf>.

⁷ The scope of the ICO Letter is not limited to the Required Access Arrangements but also considers disclosures to the SEC in some other contexts. So far as we are aware, the ICO has not subsequently made any public statement contradicting or otherwise modifying the views expressed in the ICO Letter.

that such transfers are necessary for important reasons of public interest which are recognised in UK domestic law.⁸

2. **OPINION**

2.1 Subject to the points made below, we think there are strong arguments that SCB can cooperate with the SEC in the Required Access Arrangements, including disclosing Covered Records to the SEC, without breach of UK data protection or banking confidentiality law. Furthermore, we think the risk of adverse enforcement action by the ICO is low.

2.2 However, the nature of the UK's data protection regime is that neither: (i) SCB's U.S. legal obligation to disclose Covered Records to the SEC; nor (ii) the purposes for which the SEC will require disclosure of Covered Records from the SCB provide an *absolute* justification for disclosure of *personal* data (see paragraph 3.2.1 below) to the SEC.

2.3 In particular:

2.3.1 In this memorandum (particularly in paragraph 6, but also in paragraph 5, below), we identify various requirements which must be met by SCB if its disclosures of personal data within the Covered Records are to be lawful. These requirements, however, are relatively straightforward and will apply in similar ways to a wide range of SCB's disclosures and other processing of personal data. We assume that they will be met.

2.3.2 We have also (in paragraph 5.7 below) made various assumptions about the nature of the requests for disclosure that will be made by the SEC, the U.S. legal and regulatory regime that will apply to personal data contained within the Covered Records when they are in the hands of the SEC and the SEC's related practice. These assumptions address, principally, matters of U.S. law and regulation (including regulatory practice) on which we are not qualified to

⁸ See the discussion of this derogation from the UK restrictions in paragraphs 5.1.4, 5.6 and 5.7.1(a) and (b) and 5.7.2(a) to (f) below. The ICO's conclusion is subject to the possibility that a regulated firm may in the future be in a position to put in place "appropriate safeguards" to protect personal data transferred to the SEC, in which case it would rely on those safeguards (rather than the public interest justification referenced in the ICO Letter), to allow transfers to the SEC to go ahead lawfully (see paragraph 5.6.4 below). The ICO Letter does not deal in detail with the other restrictions and requirements discussed in this memorandum (that is, restrictions and requirements under UK data protection law other than the specific restrictions on the *international transfer* of personal data, such as the lawful basis of processing). However, we interpret the absence of any reference by the ICO to such restrictions as evidence that the ICO would consider that any such restrictions would be capable of being adequately addressed so as to allow disclosures to the SEC to go ahead in compliance with UK data protection law.

express a view, but we note that, according to the ICO Letter, the ICO has discussed them with the SEC and concluded that they are satisfied. In our view this provides very substantial comfort that the ICO, at least, will consider any such disclosures to be lawful.

2.3.3 There remains the possibility, in relation to any given requested disclosure of personal data, that the ICO or an English court might take a view that SCB's and the SEC's interests in the disclosure going ahead are overridden by the interests or fundamental rights and freedoms of the individuals to whom the disclosed personal data relate. We discuss this possibility further in paragraphs 5.7.2(i) to (r) of this memorandum. It will be necessary for SCB to make a case-by-case assessment of each request for disclosure (unless it does not require disclosure of *personal* data) in order to satisfy itself that this is not the case. Given the strong public interest in disclosure, however, and taking into account the views expressed by the ICO in the ICO Letter, it is unlikely in our opinion that these considerations will prevent disclosure provided the SEC is willing to consider and address in good faith any proposals from SCB to redact from Covered Records any material personal data which are not relevant to / required for the purposes of carrying out the SEC's relevant functions (for example, where a particular document, containing pertinent material, also includes personal data of a relatively sensitive nature which are not relevant given the subject matter of the request).

2.3.4 Although the nature of SCB's UK legal obligations is that there will inevitably be some uncertainty as to the lawfulness of some particular requested disclosures of personal data pursuant to the Required Access Arrangements, the views expressed by the ICO in our view provide very substantial comfort that the ICO will not take a contrary view or, even if it did, seek to impose sanctions on SCB where it makes such disclosures as envisaged in the ICO Letter. Although this leaves open the possibility of individuals seeking compensation through the English courts for breach of UK data protection law, arguing that particular disclosures are unlawful, such claims – even if successful - would not actually prevent disclosure.

3. RELEVANT APPLICABLE LAW

3.1 In this memorandum, we consider potential requirements and restrictions arising under English law in relation to the Required Access Arrangements in two categories:

3.1.1 UK data protection law – see paragraphs 3.2 and 4 to 6 below; and

3.1.2 the English law of confidence – see paragraphs 3.3 and 7 below.

3.2 UK data protection law comprises, for relevant purposes:

3.2.1 EU General Data Protection Regulation 2016/679, as transposed into UK law and amended following the expiry of the Brexit transitional period by the European Union (Withdrawal) Act 2018 and a related statutory instrument (the "**UK GDPR**"); and

3.2.2 the UK Data Protection Act 2018, as similarly amended (the "**UK DPA**").⁹

The UK GDPR and UK DPA regulate the "processing"¹⁰ of "personal data" (that is, information relating to identified or identifiable living individuals, known as "data subjects"). The UK GDPR and UK DPA do not apply to processing of information relating to corporate persons except where the information also relates to individuals. The Covered Records will extremely likely include personal data relating to SCB's own employees, employees of and other individuals associated with SCB's customers and other counterparties and other individuals. The UK GDPR and UK DPA will create rights of these individuals which are not dependent on their having relationships of particular kinds with SCB. They impose a series of requirements and restrictions on any person who acts as a "controller" or a "processor" in relation to the processing of personal data. A "controller" is a person who determines the purposes and means of processing of personal data. A "processor" is a person who processes personal data on behalf of a controller. In respect of the storage, and any disclosure or other processing forming part of the Required Access Arrangements, of personal data contained within the Covered Records, SCB will act as a controller.¹¹

3.3 While England does not have a statutory banking secrecy regime, the English courts have created¹² an implied duty of confidence which is owed in certain circumstances, including (in most circumstances) by financial institutions to their clients and other counterparties and by employers to their employees. The duty of confidence prohibits misuse of information of confidential nature which is obtained from or in the course of

⁹ The UK GDPR and UK DPA were both amended by statutory instrument, with effect from the end of the Brexit transitional period, in various respects so that they continue to apply effectively in UK law when the UK is no longer a member state of the EU.

¹⁰ Which, pursuant to article 4(2) of the UK GDPR, includes the "*disclosure by transmission, dissemination or otherwise making available*" of personal data.

¹¹ The terms "**personal data**", "**data subject**", "**processing**", "**controller**" and "**processor**" are all defined in article 4 of the UK GDPR.

¹² The leading case in the banking context is *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.

dealing with the relevant person, including prohibiting disclosure except with consent or in other specified circumstances, further discussed in paragraph 7 below.

4. INTRODUCTION TO DATA PROTECTION ISSUES

4.1 UK data protection law imposes a series of requirements and restrictions on controllers such as SCB in respect of their disclosure or other processing of personal data, including, in SCB's case, the personal data within the Covered Records.

4.2 In paragraph 5 below, we consider UK data protection requirements and restrictions of a relatively fundamental nature, which might in principle restrict or even prevent SCB from lawfully cooperating in the Required Access Arrangements. In paragraph 6 we briefly discuss less fundamental requirements and restrictions, which will or may arise in respect of SCB's processing of personal data for the purposes of the Required Access Arrangements but which in our opinion should not give rise to fundamental difficulties.

5. FUNDAMENTAL ISSUES – REQUIREMENTS AND RESTRICTIONS THAT COULD IN PRINCIPLE MAKE THE PROPOSED ARRANGEMENTS UNLAWFUL

5.1 Introduction

The key relevant issues arise under articles 6, 9 and 10, and Chapter V, of the UK GDPR. In particular:

5.1.1 *lawful basis for disclosure*: **article 6** of the UK GDPR prohibits all disclosure or other processing of personal data unless it satisfies one of a defined set of what are known as "**lawful bases**" of processing as set out in article 6(1) of the UK GDPR – any disclosure or other processing of personal data for the purposes of the Required Access Arrangements will therefore be prohibited unless it fits within one of these lawful bases;

5.1.2 *disclosure of special category data*: **article 9** of the UK GDPR prohibits all disclosure or other processing of personal data in certain particularly sensitive categories (known as "**special category data**")¹³ unless, in addition to satisfying an article 6 lawful basis, the processing satisfies one of a defined set of

¹³ The special categories cover: (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; (ii) genetic data; (iii) biometric data processed for the purpose of uniquely identifying a natural person; (iv) data concerning health; and (v) data concerning a natural person's sex life or sexual orientation. We note that the ICO Letter takes the view that some personal data in these categories are likely to be disclosed to the SEC within the scope of the Required Access Arrangements, a position with which we would agree.

conditions as set out in article 9(2) of the UK GDPR and further clarified by section 10 of the UK DPA and schedule 1 to the UK DPA ("**DPA Schedule 1**") – any disclosure or other processing of special category data for the purposes of the Required Access Arrangements will therefore be prohibited unless it meets one of these conditions;

5.1.3 ***disclosure of criminal offence data***: **article 10** of the UK GDPR prohibits all disclosure or other processing of personal data relating to criminal convictions and offences or related security measures¹⁴ ("**criminal offence data**") unless, in addition to fitting with an article 6 lawful basis, the processing satisfies one of a defined set of conditions set out in in DPA Schedule 1 – any disclosure of other processing of criminal offence data will therefore be prohibited unless it meets one of these conditions; and

5.1.4 ***international transfer of personal data***: **Chapter V** (and in particular **article 44**¹⁵) of the UK GDPR prohibits transfer of personal data to countries or territories outside the UK unless, in addition to the transfer satisfying an article 6 lawful basis (and, if relevant, additionally satisfying an article 9 and/or 10 condition), one of the following provisions applies (each of which must be applied in a cascading / 'waterfall' manner):

(a) pursuant to article 45 of the UK GDPR and/or section 17A of the UK DPA, the relevant country or territory, or one or more (relevant)

¹⁴ By virtue of section 11(2) of the UK DPA, this includes personal data relating to "*the alleged commission of offences by the data subject, or ... proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.*" ICO guidance (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/#what>) defines criminal offence data as including "*unproven allegations; information relating to the absence of convictions*" and "*civil measures which may lead to a criminal penalty if not adhered to*". Again, we note that the ICO Letter takes the view that some criminal offence data is likely to be to the SEC within the scope of the Required Access Arrangements, a position with which we would agree.

¹⁵ For completeness, we note that article 48 of the EU GDPR, which deals with the status of transfers required by judgments of third country courts or orders of third country regulatory authorities (and which consequently may have materially impacted this analysis), is not applicable. Specifically, it was never part of the EU GDPR as it applied (as an EU Regulation with direct applicability) in the UK during the UK's membership of the EU (by virtue Article 2 of Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice), was not included in the UK GDPR (by virtue of Paragraph 41 of Schedule 1 of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) and therefore does not form part of UK data protection law.

specified sectors within it, has been determined to ensure adequate protection for personal data for the purposes of UK data protection law;

- (b) if no such adequacy decision has been granted, "**appropriate safeguards**" of various kinds, specified in articles 46 and 47 of the UK GDPR,¹⁶ are in place to protect the transferred data; or
- (c) if no appropriate safeguard is available, one of a series of derogations for specific situations, specified in article 49 of the UK GDPR, applies.

This will apply to the transfer of personal data to the SEC in the U.S., including granting the SEC access to personal data for subsequent transfer to the U.S., which would be prohibited in the absence of one of these provisions applying.

5.2 Note that the requirements of articles 6, 9 and 10, and Chapter V, of the UK GDPR are *cumulative* - meeting one of these requirements does not exempt SCB from the requirement to meet another, if it applies given the nature of the personal data, the disclosure or other processing. For example, transfer of criminal offence data to SEC in the U.S. would have to meet requirements of articles 6 *and* 10 *and* Chapter V, although not article 9, of the UK GDPR.

5.3 We briefly discuss the lawful basis requirements of article 6 of the UK GDPR in paragraph 5.4 below, the requirements relating to special category data and criminal offence data together, in paragraph 5.5, and Chapter V of the UK GDPR's restrictions on the international transfer of personal data in paragraph 5.6. We then go on, in paragraph 5.7, to consider how these requirements and restrictions can be met by SCB's disclosure or other processing of personal data for the purposes of the Required Access Arrangements.

5.4 Lawful basis of processing – article 6 of the UK GDPR

5.4.1 Article 6(1) of the UK GDPR identifies six lawful bases on which the disclosure or other processing of personal data may be justified. Any processing not able to rely upon one of these lawful bases is prohibited.

5.4.2 We set out the six available lawful bases in Part I of Annex A to this memorandum. In Part II of Annex A we briefly discuss the first five available lawful bases, none of which, in our view, would likely be suitable to justify

¹⁶ We note in passing that it is not possible for a controller such as SCB to take the view that alternative safeguards of its own (or the SEC's) devising are "*appropriate*" to protect the transferred personal data. Rather, only safeguards in the specific categories identified in article 46 of the UK GDPR can be relied upon.

disclosure or other processing of personal data in the course of cooperation with the Required Access Arrangements, other than in exceptional circumstances.

5.4.3 In our view, therefore, the necessary disclosure and other processing can only (generally) be justified on the basis of the remaining sixth lawful basis, set out in article 6(1)(f) of the UK GDPR, namely that the disclosure or other processing is necessary for the purposes of legitimate interests pursued by SCB, the SEC and/or other persons which are not overridden by the interests or fundamental rights and freedoms of the affected data subjects which require protection of personal data. We discuss this lawful basis further in paragraph 5.7 below.¹⁷

5.5 Disclosure of / granting access to special category data or criminal offence data – articles 9 and 10 of the UK GDPR

Special category data

5.5.1 Article 9(2) of the UK GDPR identifies ten conditions, at least one of which must be met for any disclosure or other processing of special category data to be justified. Any processing of special category data not able to rely upon one of these conditions is prohibited.

5.5.2 We set out the ten conditions in Part A of Annex B to this memorandum. In Part II of Annex B we briefly discuss nine of the ten conditions, none of which, in our view, would likely be suitable to justify disclosure or other processing of special category data in the course of cooperation with the Required Access Arrangements, other than in exceptional circumstances.

5.5.3 In our view, therefore, any necessary disclosure or other processing of special category data can only (generally) be justified on the basis of the remaining condition, set out in article 9(2)(g) of the UK GDPR, namely that the disclosure or other processing is (broadly speaking) necessary on substantial public interest grounds.

5.5.4 Section 10(3) of the UK DPA provides that disclosure or other processing relying on article 9(2)(g) of the UK GDPR would only meet this condition if it meets one of the conditions set out in part 2 of DPA Schedule 1.

¹⁷ See in particular paragraphs 5.7.1(e) and (f) and 5.7.2(i) to (r) below.

Criminal offence data

- 5.5.5 Article 10 of the UK GDPR prohibits all processing (including disclosure) of criminal offence data except where the processing is authorised by UK domestic law.¹⁸
- 5.5.6 Section 10(5) of the UK DPA provides that disclosure or other processing of criminal offence data pursuant to article 10 of the UK GDPR would only be considered to be authorised by UK domestic law if it meets one of the conditions set out in parts 1, 2 and 3 of DPA Schedule 1.
- 5.5.7 In our view, the conditions in parts 1 and 3 of DPA Schedule 1 will not apply to any disclosure or other processing of criminal offence data in the course of cooperation with the Required Access Arrangements, other than in exceptional circumstances.¹⁹

Considerations applicable to both special category data and criminal offence data

- 5.5.8 In effect, subject to a variation which is specified within DPA Schedule 1 (and discussed briefly in paragraph 5.5.9 below), the requirements applicable to disclosure or other processing of special category data and/or criminal offence data are the same: in each case, one of the conditions in part 2 of DPA Schedule 1 must be met.
- 5.5.9 Part 2 of DPA Schedule 1 sets out 23 conditions any of which, if met, will justify disclosure or other processing of special category data or criminal offence data. In our view, however, only three of these conditions are (other than in exceptional circumstances) capable of application to disclosure or other processing for the purposes of the Required Access Arrangements.

These conditions are as follows:

¹⁸ Processing is also authorised where carried out "*under the control of official authority*", but that will not apply in the circumstances considered by this memorandum.

¹⁹ In particular, the conditions in paragraphs 33(a) and (c) of part 3 of DPA Schedule 1, which allow processing of criminal offence data which is "*(a) necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), ...or ... (c) ... otherwise ... for the purposes of establishing, exercising or defending legal rights*", are likely to be interpreted relatively broadly (so as, for example, to apply to administrative as well as court proceedings), and may justify some disclosures to the SEC (where they are made in the context of administrative proceedings brought, or where there is a concrete and specific likelihood of their being brought, against SCB or a third party), but will not allow all likely required disclosures in the course of cooperation with the Required Access Arrangements.

(a) ***condition 10 : preventing or detecting unlawful acts:***

This condition is met if:

- (i) the processing is necessary for the purposes of the prevention or detection of an unlawful act (including a failure to act);
- (ii) it must be carried out without the consent of the data subject so as not to prejudice those purposes;
- (iii) it is necessary for reasons of substantial public interest;²⁰ and
- (iv) SCB has an appropriate "policy document" in place, meeting the requirements of paragraph 39 of part 4 of DPA Schedule 1.²¹

(b) ***condition 11: protecting the public against dishonesty:***

This condition is met if:

- (i) the processing is necessary for the exercise of a function intended to protect members of the public against:
 - (A) dishonesty, malpractice or other seriously improper conduct;
 - (B) unfitness or incompetence;
 - (C) mismanagement in the administration of a body or association, or
 - (D) failures in services provided by a body or association;
- (ii) it must be carried out without the consent of the data subject so as not to prejudice the exercise of that function;
- (iii) it is necessary for reasons of substantial public interest;²² and

²⁰ This third sub-condition does not apply to disclosure or other processing of criminal offence data.

²¹ There is an exception to the obligation to have an appropriate policy document in place, but in our view it will not apply in the circumstances discussed in this memorandum.

²² This third sub-condition does not apply to disclosure or other processing of criminal offence data.

- (iv) again, SCB has an appropriate "policy document" in place.²³
- (c) ***condition 12: regulatory requirements relating to unlawful acts and dishonesty etc.:***

This condition is met if:

- (i) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity²⁴ which involves a person taking steps to establish whether another person has:
 - (A) committed an unlawful act (or failure to act), or
 - (B) been involved in dishonesty, malpractice or other seriously improper conduct,
- (ii) in the circumstances, SCB cannot reasonably be expected to obtain the consent of the data subject to the processing;
 - (A) the processing is necessary for reasons of substantial public interest;²⁵ and
 - (B) again, SCB has an appropriate "policy document" in place.²⁶
- (iii) Sub-conditions (A) (which only applies to disclosure or other processing of *special category*, not *criminal offence*, data) and (B) (which applies to personal data in both categories) are the same in each case.

The meaning of sub-condition (ii) to conditions 10 and 11 is unclear, and not subject to any helpful regulatory or judicial guidance, but in our view it can only reasonably be read as meaning the same as the

²³ See footnote 21 above.

²⁴ This condition can also be applied on an alternative basis, where the requirement is "*imposed by legislation or by a person in exercise of a function conferred by legislation*". In our view, however, the references to "legislation" are to UK domestic legislation and do not, therefore, cover the circumstances discussed in this memorandum.

²⁵ This third sub-condition does not apply to disclosure or other processing of criminal offence data.

²⁶ See footnote 21 above.

equivalent sub-condition to condition 12 – namely, that in the circumstances it is not reasonable to expect SCB to seek consent.

We discuss these conditions further in paragraph 5.7 below.²⁷

5.6 Restrictions on the international transfer of personal data – Chapter V of the UK GDPR

The restrictions

5.6.1 As discussed in paragraph 5.1.4 above, Chapter V of the UK GDPR restricts the transfer of personal data to third countries, and in our view the restrictions will apply not only to direct transfer by SCB to the SEC in the U.S., but also to disclosure by SCB to the SEC in the UK in circumstances where SCB anticipates that the data will subsequently be transferred to the U.S. (a so-called "onward transfer").²⁸

Adequacy determination

5.6.2 As at the date of this memorandum, the U.S. has not been determined to ensure adequate protection for personal data for the purposes of article 45 of the UK GDPR. However, it should be noted that the U.S. appears on the list²⁹ of third countries which the UK government considers as priority candidates for an adequacy determination.

5.6.3 Chapter V of the UK GDPR will therefore prohibit disclosures of personal data to the SEC for the purposes of the Required Access Arrangements (unless and until an UK adequacy determination is made which covers such transfers) unless appropriate safeguards are in place to protect the transferred personal data or one of the derogations for specific situations allowing transfer without appropriate safeguards applies.

²⁷ See in particular paragraphs 5.7.1(c), (d), (g) and (h) and 5.7.2(b), (g), (h), (s) and (t).

²⁸ The restrictions will *not* in our view apply if the SEC merely inspects personal data in the UK and does not transfer them to the U.S. We assume, however, that this is a relatively unlikely eventuality and, for the purposes of the remainder of this memorandum, we therefore assume that any relevant disclosure of personal data to the SEC will be subject to the restriction contained within Chapter V of the UK GDPR.

²⁹ See <https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation> (25 August 2021). Even if a UK adequacy determination is reached for the U.S., however, it may be limited to particular sectors and will not therefore necessarily apply to transfers to the SEC.

Appropriate safeguards

5.6.4 The UK GDPR allows international transfers based only on certain specific kinds of appropriate safeguard:

- (a) One possibility would be for the transfers to be subject to a legally binding and enforceable instrument protecting the data, entered into between public authorities or bodies (e.g. between the FCA and the SEC) pursuant to article 46(2)(a) of the UK GDPR. So far as we are aware, however, no such instrument is in place that would apply to relevant transfers by SCB to the SEC, and of course it is not within SCB's power to put such an instrument in place.³⁰
- (b) The only other realistic possibility would be for the transfers to be made on the basis of a data transfer agreement between SCB and the SEC which is in a form approved for the purposes of the UK GDPR pursuant to either article 46(2)(c) or article 46(2)(d) of the UK GDPR (one such form of agreement is approved, and the ICO is currently consulting on the possibility of replacing it with one or more other forms of agreement).

In such case, based on article 46(1) of the UK GDPR and the decision of the European Court of Justice³¹ in the *Schrems II* case,³² it would also be necessary for SCB to satisfy itself that the effect of the relevant agreement would be to make enforceable data subject rights and effective legal remedies available to the subjects of the transferred data – in particular, that the agreement would be enforceable against the SEC in the U.S., and that U.S. law and regulation would not create rights of access to or interference with the data for U.S. governmental agencies

³⁰ It is also unclear whether it would be possible for a legally binding and enforceable instrument between public authorities or bodies to allow international transfers made by private sector third parties to the instrument (such as SCB). Since (so far as we are aware) no such instrument is in place, however, we have not considered this point in detail for the purposes of this memorandum.

³¹ Although *Schrems ii* is a decision of the European Court of Justice, which is an EU institution, as the decision was reached during the Brexit transitional period it forms part of English law regarding interpretation of the UK GDPR by virtue of the European Union (Withdrawal) Act 2018. This is borne out by the wording of Article 49 of the UK GDPR which states "In the absence of ... appropriate safeguards pursuant to Article 46".

³² *Data Protection Commissioner v. Facebook Ireland Ltd.* Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).

(or others) that would be inconsistent with the fundamental data privacy principles of English law.

(c) We note that:

- (i) the ICO Letter encourages exporting controllers to seek to enter into such agreements with the SEC, and only to rely on a derogation if they are unable to do so (or until they have succeeded in doing so); and
- (ii) generally, the European data protection supervisory authorities have taken the view, in their published guidance³³ that a controller or processor can only rely on a derogation where it is not feasible to put in place appropriate safeguards.

We understand that SCB has not entered into such an agreement with the SEC, however, and we assume that the SEC would not in practice be willing to enter into such an agreement with SCB. Whilst SCB should confirm this point with the SEC, we therefore assume that it will not be feasible to put appropriate safeguards in place and that SCB must (and can) rely on a derogation, allowing it to disclose personal data to the SEC without appropriate safeguards (and, in particular, without the need for a *Schrems II* analysis).

Derogations under article 49 of the UK GDPR

5.6.5 Article 49 of the UK GDPR identifies eight derogations, one of which would need to apply, in the absence of an adequacy determination or appropriate safeguards, for any transfer of personal data to a country or territory outside the UK to be justified. All other such transfers are prohibited.

5.6.6 We set out the eight available derogations in Part I of Annex C to this memorandum. In Part II of Annex C, we briefly discuss seven of the available derogations, none of which, in our view, will be suitable to justify disclosure of personal data to the SEC for the purposes of the Required Access Arrangements other than in exceptional circumstances.

5.6.7 In our view, therefore, the necessary disclosures can only (generally) be justified on the basis of the other derogation, set out in article 49(d) of the UK GDPR,

³³ See for example the European Data Protection Board's *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, which remain persuasive for the purposes of English law as they were published, with the participation of the ICO, before the UK left the European Union.

namely that the international transfer is necessary for important reasons of public interest, and the relevant public interest is recognised in UK domestic law. We discuss this lawful basis further in paragraph 5.7 below.³⁴

5.7 How relevant processing will meet the requirements and restrictions of articles 6, 9 and 10, and Chapter V, of the UK GDPR

5.7.1 Summarising our conclusions reached in paragraphs 5.4 to 5.6 above, and addressing issues in what seems to us to be a convenient order from the perspective of ease of exposition, any given disclosure of personal data to the SEC for the purposes of the Required Access Arrangements will be prohibited unless all of the following eight conditions are met³⁵:

Public interest conditions

- (a) the disclosure is necessary for important reasons of public interest (see paragraph 5.6.7 above);
- (b) the relevant public interest is recognised in UK domestic law (also paragraph 5.6.7);
- (c) if the disclosure is of *special category data* (but not otherwise), it is necessary for reasons of substantial public interest (paragraph 5.5);
- (d) if the disclosure is of either *special category data* or *criminal offence data* (but not otherwise), it is necessary for one or more of the following purposes (also paragraph 5.5):
 - (i) the prevention or detection of an unlawful act (including a failure to act);
 - (ii) the exercise of a function intended to protect members of the public against: (1) dishonesty, malpractice or other seriously improper conduct; (2) unfitness or incompetence; (3) mismanagement in the administration of a body or association, or (4) failures in services provided by a body or association; or
 - (iii) complying with, or assisting other persons to comply with, a requirement forming part of generally accepted principles of

³⁴ See in particular paragraphs 5.7.1(a) and (b) and 5.7.2(a) to (f).

³⁵ Or are not applicable, in the cases of the conditions set out in paragraphs 5.7.1(c), (d), (g) and (h), which only need to be met in cases of disclosure (or other processing) of special category and/or criminal offence data.

good practice relating to a type of body or an activity which involves a person taking steps to establish whether another person has: (1) committed an unlawful act (or failure to act); or (2) been involved in dishonesty, malpractice or other seriously improper conduct;

Legitimate interests

- (e) the disclosure is necessary for the purposes of legitimate interests pursued by SCB, the SEC or another person (paragraph 5.4);
- (f) those interests are not overridden by the interests or fundamental rights and freedoms of the affected data subjects which require protection of personal data (also paragraph 5.4);

Miscellaneous

- (g) if the disclosure is of either ***special category data*** or ***criminal offence data*** (but not otherwise), it must be carried out without the consent of the data subject so as not to prejudice the relevant purpose specified in paragraph 5.7.1(d) above (paragraph 5.5); and
- (h) if (again) the disclosure is of either ***special category data*** or ***criminal offence data*** (but not otherwise), SCB has an "appropriate policy document" in place (also paragraph 5.5).

5.7.2 We consider the application of these conditions to disclosure for the purposes of the Required Access Arrangements, in turn, as follows:

Public interest conditions

- (a) The public interest conditions break into two categories:
 - (i) the general conditions identified in paragraphs 5.7.1(a) to (c) above (see paragraphs 5.7.2(b) to (g) below); and
 - (ii) the more specific conditions identified in paragraph 5.7.1(d) (see paragraph 5.7.2(h))

General public interest conditions

- (b) We have considered the question of whether it is possible for a person other than the legislature or courts or a public authority to adduce, or reach a view, as to whether a particular disclosure or other act serves a

public interest. In our view, this *is* possible, particularly given the approach taken by the UK GDPR – that is, the relevant public interest needs to be recognised in UK domestic law, which allows SCB (and its advisors) to identify them objectively by reference to the law. Recognition in UK domestic law does not necessarily need to be in legislation. It could be referenced in case law or in statements from public authorities (such as the ICO Letter).³⁶

- (c) The ICO Letter considers whether disclosures for the purposes of the Required Access Arrangements will meet the general public interest conditions identified in paragraphs 5.7.1(a) and (b) above and concludes that they will. We understand that this conclusion was reached in discussion with the FCA (as well as the SEC itself) and, subject to the points discussed in paragraphs 5.7.2(d) and (f) below, we agree with it. We reach this conclusion on the following basis:
 - (i) Disclosures to the SEC in the context of the Required Access Arrangements are made for the purposes of ensuring the proper legal administration of SCB (as an SEC-regulated firm) and preventing, detecting and/or prosecuting (or taking other enforcement action in respect of) money-laundering, fraud, sanction evasion and other unlawful behaviour – this includes both behaviour in relation to finance which is unlawful under UK law and conduct in the U.S. that would amount to such unlawful behaviour if carried out in the UK.
 - (ii) There are *important public interests* in pursuing these purposes – to the extent that this is not self-evident, it is indicated by the considerations in paragraph 5.7.2(c)(iii) below.
 - (iii) These public interests are *recognised in UK domestic law* – in particular, through:
 - (A) the UK's participation (as signatory), through HM Treasury, the Bank of England and the FCA, in the Financial Stability Board (in which the U.S. / SEC also participate), an international body dedicated to the fostering of sound, stable and well-functioning financial systems (including the fight against financial crime),

³⁶ See Recital 41 to the UK GDPR and related ICO guidance (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/>).

whose compendium of standards, including the IOSCO Objectives and Principles of Securities Regulation and IOSCO Administrative Arrangement relating to the transfer of personal data, are consistent with the SEC's own rules and regulations and deal specifically with examination of regulated firms by regulated bodies;³⁷

- (B) section 1(D) of the UK Financial Services and Markets Act 2000 ("**FSMA**"), which identifies, as an objective of FSMA, preventing the UK financial system (including the firms within it, such as SCB) from being used for purposes connected with financial crime, including conduct overseas which would be criminal if conducted in the UK; and
 - (C) SCB's general obligation under Principle 11 of the FCA handbook to deal with its regulators, including overseas regulators such as the SEC, in an open and cooperative way.
- (iv) Assuming that:
- (A) the SEC, as a matter of practice, makes *targeted* requests for information which includes personal data, based on risk and related to specific clients and accounts and/or employees, rather than systematic and large scale requests; and
 - (B) SCB, in response to each request:
 - (1) satisfies itself that the SEC is acting within the scope of its regulatory authority;
 - (2) considers whether, where records containing material personal data ³⁸ are requested, those

³⁷ We note in particular that the IOSCO Objectives and Principles include:

- "10. The Regulator should have comprehensive inspection, investigation and surveillance powers."
- "12 The regulatory system should ensure an effective and credible use of inspection, investigation, surveillance and enforcement powers and implementation of an effective compliance program."

³⁸ For example, special category data, criminal offence data and/or significant data relating to individuals in their private rather than their business capacities.

personal data are in practice likely to be needed given the context of the request, and, where practicable, proposes redactions to remove material personal data which are not relevant in the context of the request (but acknowledging that ultimately it will be for the SEC to decide whether redaction is acceptable); and

- (3) keeps an appropriate record of these considerations and proposals, which could be used as evidence if, for example, a complaint was made and the ICO asked for an explanation,

disclosures for the purposes of the Required Access Arrangements will, in our opinion, be *necessary* for the purposes of those public interests.

- (d) Our conclusion in paragraph 5.7.2(c) above is based on assumptions about the SEC's authority, and the manner in which the SEC exercises that authority, which are matters of U.S. law and regulatory practice on which we are not expressing a view for the purposes of this memorandum. This applies in particular to:
 - (i) the points made in paragraph 5.7.2(c)(i) regarding the purposes for which the SEC requests disclosures in the context of the Required Access Arrangements;
 - (ii) the point made in paragraph 5.7.2(c)(iii)(A) regarding consistency between the SEC's rules and regulations and the IOSCO Objectives and Principles of Securities Regulation; and
 - (iii) the point made in paragraph 5.7.2(c)(iv)(A) regarding the practices adopted by the SEC in the exercise of its powers.
- (e) If any of these assumptions does not hold good in relation to a particular requested disclosure, the public interest conditions may not be met. In practice, however, very substantial comfort on this point can in our view be derived from the ICO Letter. In particular, the risk of the ICO taking an adverse view on this point in relation to a disclosure of personal data made in the context of the Required Access Arrangements is in our view low.

- (f) We do note the possibility that the SEC might exercise its powers to seek personal data from the SCB in the context of an investigation into alleged conduct which is unlawful under U.S. law but would not be unlawful if carried out in the UK.³⁹ In those circumstances, in our view, the general public interest conditions would not be met and disclosure of personal data in response to the SEC's request would be unlawful.
- (g) Although the general public interest conditions come in two varieties (see paragraphs 5.7.1(a) to (c): *important* reasons of public interest, *recognised in UK domestic law* (in relation to transfers to third countries) *versus* reasons of *substantial* public interest (in relation to processing of special category data)), in our view they cannot reasonably be interpreted as setting two different tests – we can see no policy reason why the public interest underpinning processing of special category data would need to meet a different standard to the public interest underpinning transfer to a third country without adequate protection / safeguards, and, in particular, we cannot identify any basis for distinguishing between an "important" and a "substantial" public interest.⁴⁰ We therefore take the view that the condition identified in paragraph 5.7.1(c) will be met if the conditions identified in paragraphs 5.7.1(a) and (b) are met. The condition identified in paragraph 5.7.1(c) does not, therefore, require separate consideration.

Specific public interest conditions

³⁹ Here we are referring to fundamental differences of approach between the U.S. and UK regimes. Where differences arise merely because of different approaches to detailed regulation of the same issue, in our view the public interest condition will be met.

Note, further, that this issue does not turn on the nature of the data sought from SCB, nor on whether SCB or any of its employees is itself (or themselves) accused of carrying out or has actually carried out an unlawful act under U.S. or UK law, but rather on the reason for the request for disclosure from the SEC – if the SEC is pursuing an objective which is not recognised as being in the public interest in UK law, the public interest condition will not be met.

⁴⁰ It may be arguable that the condition set out in paragraph 5.7.1(c) in relation to processing of special category data sets a lower standard than the conditions set out in paragraphs 5.7.1(a) and (b) in relation to transfer to a third country, allowing reliance on a public interest which is not recognised in UK domestic law, but in any case the paragraph 5.7.1(c) condition will in our view be met if the paragraphs 5.7.1(a) and (b) conditions are met, even if not *vice versa*. In practice it is likely that the minor differences in language between the two sets of public interest conditions arise from their different legislative origin – the conditions identified in paragraphs 5.7.1(a) and (b) form part of the UK GDPR, based on the EU GDPR; whereas the condition identified in paragraph 5.7.1(c) forms part of the UK DPA and uses language based on the UK domestic legislation which was replaced by the EU GDPR and UK DPA in 2018.

- (h) The specific public interest conditions (see paragraphs 5.5 and 5.7.1(d) above) require, in addition, that, where special category data or criminal offence data are to be disclosed, the disclosure must be necessary for one of the specific purposes set out in paragraph 5.7.1(d). Given the purposes for which we are assuming that the SEC exercises its authority, however, we take the view that this condition will be met where disclosures are made for the purposes of the Required Access Arrangements. Broadly speaking, disclosures will be made for the purposes of preventing or detecting⁴¹ (finance-related) unlawful acts. They may on occasion be made for somewhat wider purposes, but in those cases they would be made for the purpose identified in paragraph 5.7.1(d)(ii) or, perhaps in limited cases, 5.7.1(d)(iii).⁴² This, however, is subject to the same assumptions and possible exceptions as are set out in paragraphs 5.7.2(d) and (f) in relation to the general public interest conditions.

Legitimate interests condition

- (i) The legitimate interests condition requires any disclosure of personal data by SCB to the SEC for the purposes of the Required Access Arrangements to meet three tests:
- (i) the disclosure must serve a legitimate interest pursued by SCB, the SEC or another person;

⁴¹ In our view, steps taken in order to *investigate or sanction past* unlawful acts should for these purposes reasonably be regarded as taken in order to *prevent future* unlawful acts, on the basis that part of the purpose of investigation and punishment is to deter others from committing similar unlawful acts in future. A similar analysis applies to protecting the public against malpractice, etc.: steps taken to investigate or sanction past malpractice should reasonably be regarded as taken in part in order to protect the public against future malpractice.

⁴² The structure of the UK GDPR and UK DPA (in relation to special category data) is in our view relevant here. The starting point, in article 9(2)(g) of the UK GDPR, is that (assuming it satisfies an article 6 lawful basis) disclosure or other processing of special category data is permitted if it is necessary for reasons of substantial public interest. Article 9(2)(g) of the UK GDPR goes on to require UK domestic law to provide a basis for the processing and part 2 of DPA Schedule 1 does so. Part 2 of DPA Schedule 1 in our view needs to be read in the context of the relatively broad drafting of article 9(2)(g) of the UK GDPR, the overall objective of the legislation being to allow processing of special category data which is necessary for reasons of substantial public interest. The specific public interest conditions should therefore not be read narrowly where the general public interest conditions are met.

- (ii) it must actually be necessary for the purposes of that legitimate interest; and
 - (iii) that legitimate interest must not be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- (j) The first and second of these tests will in our view be met where the general public interest tests are met (see paragraphs 5.7.2(b) to (g) above) – SCB has a legitimate interest in cooperating with the SEC to pursue the important public interests discussed in those paragraphs, and we have already concluded, subject to assumptions and exceptions, that the relevant disclosures are necessary for the purposes of those public interests.
- (k) Although the ICO Letter identifies the need for any disclosure to the SEC to satisfy an article 6 lawful basis, it does not consider which lawful basis will apply nor the factors that will need to be taken into account in deciding whether a firm's legitimate interest in making such a disclosure might be overridden by the privacy interests of the data subjects. There could clearly, at least in theory, be circumstances where the data subjects' privacy interests override. In practice, SCB will need to consider requests on a case-by-case (or category-by-category) basis and balance the public interest in disclosure (and its own interest in cooperating with the SEC and complying with its U.S. legal and regulatory obligations) against the interests and fundamental rights and freedoms of the individuals whose personal data are to be disclosed. SCB should keep a record of these assessments so that it can produce them to the ICO should a complaint be made (on this, see also paragraph 6.2.1 below).
- (l) The need to conduct this balancing test creates some inevitable uncertainty as to whether all disclosures that might be requested by the SEC in the context of the Required Access Arrangements will satisfy the legitimate interests condition. Although neither the ICO nor the EDPB (defined below) has expressed an explicit view on this point, however, in our opinion a public interest which meets the test in article 49(1)(d) of the UK GDPR (i.e. the public interest is important and recognised in UK domestic law) will provide a particularly strong legitimate interest in disclosure (or other processing), capable of being overridden by the legitimate interests of data subjects only in

exceptional circumstances, where there is severe prejudice to the interests or fundamental rights and freedoms of the data subject. In reaching this opinion we have taken into account, in particular, the intrinsically international nature of the business that SCB will be carrying out and which brings it within the jurisdiction of the SEC: in the context of the conduct of this kind of business, in our view, disclosure to competent overseas regulatory authorities, which may not be subject to legal and regulatory regimes and practices which provide all of the protections that a data subject might expect under UK domestic law and regulation (and associated practice), can be assumed to be within the reasonable contemplation of at least the large majority, and the most significant, of the data subjects.⁴³ The fact that the ICO Letter does not identify article 6 as raising fundamental issues for the Required Access Arrangements in our view provides a strong indication that the ICO would agree with this opinion.

- (m) Disclosure of personal data to the SEC, in the U.S., is likely to be somewhat prejudicial to the interests and fundamental rights and freedoms of data subjects in the sense that it deprives them of the full panoply of protection for their personal data (and associated interests) under UK law – clearly, there is no guarantee that they will receive the same level of protection under U.S. law and regulation as if their personal data remained within the UK and were handled only by UK authorities. However points made by the ICO in the ICO Letter and discussed briefly in paragraph 5.7.2(o) below do in our view provide significant comfort, both as to the actual level of protection for personal data disclosed to the SEC and, equally important, as to the view that the ICO will be minded to take if a complaint is made.
- (n) Whilst, as we have said, satisfaction of the legitimate interests condition will need to be assessed on a case-by-case or category-by-category basis, we have considered its application to likely disclosures in the context of the Required Access Arrangements and reached the following conclusions:
 - (i) It is likely that the majority of personal data within Covered Records will be relatively innocuous in nature – that is, they will relate to data subjects only in their business rather than their

⁴³ Recital 47 to the UK GDPR identifies the reasonable expectations of the data subjects as a factor to be taken into account in conducting a legitimate interests assessment.

private capacity⁴⁴ and will not suggest that the data subjects may have committed or otherwise been involved in criminal offences, regulatory breaches or other wrongdoing. In these cases, given the considerations in paragraphs 5.7.2(l) and (m) above and (o) and (p) below, we cannot see grounds for an argument that SCB's legitimate interests in disclosing the personal data are overridden by the interests or fundamental rights and freedoms of the data subjects. In these cases, in our view, the legitimate interests condition will therefore likely be satisfied.

- (ii) Some personal data within Covered Records may implicate data subjects in actual or alleged criminal offences, regulatory breaches or other wrongdoing, which fall within the scope of the SEC's regulatory oversight or, in the case of criminal offences, which the SEC would be likely to disclose to the U.S. Department of Justice. In those cases, whilst the potential for prejudice to the interests or fundamental rights and freedoms of the data subjects is real, the public interest in disclosure will be particularly strong and in our opinion it is unlikely that SCB (or the ICO, should the question come to its attention) could conclude that SCB's legitimate interests in disclosing the personal data are overridden by the interests or fundamental rights and freedoms of the data subjects. In these cases, in our view, the legitimate interests condition will therefore again be satisfied, although possibly with some limited exceptions – for example, where disclosure is particularly prejudicial to a data subject and the relevant data are of a low level of materiality from the perspective of the SEC's oversight role.
- (iii) There may be some, relatively incidental, personal data within the Covered Records which relate to individuals in their personal rather than their business capacity or, conceivably, implicate them in actual or alleged wrongdoing which is entirely outside the scope of the SEC's oversight role. These data would most likely be caught by a request for disclosure because they happen to be contained within documents which also deal with pertinent matters. In such cases, the legitimate interests condition may not

⁴⁴ Or if they do relate to a data subject in their personal capacity, they will be trivial in nature – for example, the fact that an individual is unavailable because on holiday or off sick, mentioned in passing in a business communication.

be satisfied and, in our opinion, disclosure in the context of the Required Access Arrangements may therefore be unlawful. In practice we would expect SCB to seek to agree with the SEC, on an occasional basis in relation to particular disclosure requests, that specific personal data in this category should be redacted.

- (o) The ICO Letter makes various comments about the legal and regulatory scheme to which the SEC will be subject in requesting and then using / disclosing personal data from a firm such as SCB, and the SEC's related practices. In particular, it refers to:
 - (i) the SEC's practice of making targeted requests (see paragraph 5.7.2(c)(iv)(A) above);
 - (ii) SEC examinations being non-public, information, and data and documents, being maintained in a secure manner and not disclosed except for certain uses publicly disclosed by the SEC, including an enforcement proceeding, pursuant to a lawful request of the US Congress or a properly issued subpoena, or to other regulators who have demonstrated a need for the information and provide assurances of confidentiality;
 - (iii) the information being exempt from the U.S. freedom of information regime;
 - (iv) use of information by the SEC solely for its own lawful regulatory purpose; and
 - (v) audit of the SEC by the US Government Accountability Office and other governmental oversight.

These are all matters of U.S. law, regulation and/or practice on which we do not express a view in this memorandum. We have assumed, generally, that the SEC will be subject to legal and/or regulatory requirements and/or will adopt practices which, taken together, provide appropriate protection for the personal data that it receives from SCB and, in particular, that data subjects will have legally effective rights which they can exercise against the SEC in respect of any alleged misuse of their personal data.

- (p) In considering the application of the legitimate interests lawful basis of processing to disclosures in the context of the Required Access

Arrangements, we have also taken account of the "initial" views expressed by the European Data Protection Board (the "**EDPB**")⁴⁵ in a letter (the "**LIBE Letter**") sent⁴⁶ to the LIBE committee of the European Parliament on 10 July 2019 in relation to disclosures that may be made by cloud service providers regulated by the EU data protection law to U.S. law enforcement agencies in response to disclosure demands subject to the U.S. Stored Communications Act as interpreted by the Clarifying Lawful Overseas Use of Data Act to clarify its extraterritorial application (the "**Cloud Act**").⁴⁷ Cloud Act disclosures are similar in some respects to disclosures in the context of the Required Access Arrangements, in that they are made by entities subject to European data protection law to US governmental agencies, required by U.S. law, and (generally) made for the purposes of assisting U.S. law enforcement in detecting, investigating or prosecuting actual or alleged criminal offences.

- (q) In the LIBE Letter, the EDPB acknowledges that such service providers (broadly equivalent for these purposes to SCB in the context of the Required Access Arrangements) may have legitimate interests in making Cloud Act disclosures – both interests in complying with their obligations under U.S. law (so as to avoid sanctions); and interests in furthering the interests of U.S. law enforcement. It tentatively concludes, however, that these interests will be overridden by the interests and fundamental rights and freedoms of the individuals whose personal data are disclosed, and therefore that it will not be possible for EU service providers to rely on the legitimate interests condition to form a lawful basis for Cloud Act disclosures for the purposes of the EU GDPR. This initial conclusion is reached on the basis that the affected individuals may be deprived of various protections that would be available to them under European law – for example, the ability to seek effective remedies against the U.S. recipients of their data if they are misused – and that

⁴⁵ The EDPB is a committee comprising (amongst others) representatives of the data protection supervisory authorities of the EU member states.

⁴⁶ The letter was sent jointly by the EDPB and the European Data Protection Supervisor (the "**EDPS**"), which is the supervisory authority for processing carried out by European Union institutions (which is regulated by an EU Regulation similar to the EU version of the GDPR). The EDPS does not have jurisdiction over SCB as a private sector firm.

⁴⁷ A copy of the LIBE Letter, including its annex setting out the EDPB's concerns, is available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

service providers receiving demands for disclosure would not be in a position to conduct an appropriate assessment of the possible consequences of disclosure. The EDPB notes, in particular, the various bases on which various U.S. law enforcement bodies can demand disclosure of personal data under the Cloud Act, including (in some circumstances) requiring disclosure without formal written requests or the need to show probable cause.

- (r) In our view, disclosures to the SEC in the context of the Required Access Arrangements under the UK GDPR can be distinguished from disclosures to U.S. law enforcement agencies under the Cloud Act under the EU GDPR, as understood by the EDPB in the LIBE Letter, on the following bases:
 - (i) The LIBE Letter has no formal status under the UK GDPR. It is open to the ICO and UK courts to take a different view, and we would expect them to do so. The letter is in any case expressed to present the "initial", rather than the definitive, views of the EDPB.
 - (ii) The LIBE Letter contemplates disclosures to a range of U.S. law enforcement agencies under various different U.S. legal channels. This is to be contrasted with the Required Access Arrangements, which involve disclosure by a regulated firm to the SEC for limited purposes, and subject to the protections, which have been reviewed and considered sufficient by the ICO, discussed in paragraphs 5.7.2(c) and (o) above.
 - (iii) The LIBE Letter contemplates disclosures by service providers, holding personal data on behalf of their customers, who (the service providers) will typically have no direct or indirect relationships with the individuals to whom the disclosed data relate. This is to be contrasted with the Required Access Arrangements, which involve disclosures by SCB itself of personal data relating principally to its own employees and those of its customers and other counterparties. In particular, those individuals, given their direct or indirect relationship to SCB, can in our view be assumed to have a reasonable expectation that data relating to their relevant engagements with SCB may be disclosed to the SEC (and, indeed, SCB will generally have specifically informed them that their personal data may be

disclosed to overseas regulatory authorities – see paragraph 6.2.3 below).

- (iv) Given the wide scope of potential Cloud Act disclosures, the EDPB was unable to reach the view that they would (generally) be necessary on important public interest grounds for the purposes of articles 9 and 10 and Chapter V of the EU version of the GDPR. This is to be contrasted with the Required Access Arrangements, where the ICO has taken a clear view that this condition is met. Important public interests, in our view, form a particularly strong legitimate interest in disclosure, which would be overridden only by serious prejudice to the interests or fundamental rights and freedoms of the data subjects.

On this basis, and particularly given the strong positive view expressed by the ICO (albeit not specifically in relation to article 6(1)(f)), disclosures in the context of the Required Access Arrangements can in our opinion be based on the legitimate interests condition, with the limited exceptions discussed in paragraphs 5.7.2(n)(ii) and (iii) above, despite the views tentatively expressed by the EDPB in the LIBE Letter.

Miscellaneous other conditions

- (s) ***if the disclosure is of either special category data or criminal offence data (but not otherwise), it must be carried out without the consent of the data subject so as not to prejudice the relevant purpose specified in paragraph 5.7.1(d) above:***
 - (i) This condition will in our view be met if the specific public interest conditions are met. Any requirement to obtain consent would inevitably risk prejudice to the relevant purpose, since consent could not (under the UK GDPR) be compelled and, if it was sought but withheld, the required disclosure would be unlawful.
 - (ii) We can imagine a counter-argument that the condition is not met in relation to personal data of data subjects who are willing to consent to any proposed disclosure, because it would be open to SCB to seek consent, rely on consent if it is provided, and go ahead without consent only if consent is withheld. In our view, however, a consent obtained on such a basis would not be a genuine and valid consent for the purposes of the UK GDPR – it

would not be "freely given", because the data subject would have no option of withholding consent and preventing the disclosure from going ahead.

- (t) *if the disclosure is of either special category data or criminal offence data (but not otherwise), SCB has an appropriate "policy document" in place:*

This condition is of course met if SCB has an appropriate policy document in place as required by DPA Schedule 1. We assume for the purposes of this memorandum that SCB will meet this requirement. In our experience, policy documents of this kind are typically prepared by substantial organisations which process special category data and/or criminal offence data as part of their wider UK GDPR compliance programmes. It is therefore our expectation that SCB will already have such a policy (or policies, applicable to data in different categories) in place, and the practical requirement will therefore be to check it to ensure that it is appropriate to disclosures in the context of the Required Access Arrangements. We should of course be happy to assist with review or drafting of a policy document if that would be helpful.

5.8 Conclusion

We therefore conclude that, subject to the assumptions and exceptions set out above, disclosures of Covered Records (and, specifically, any personal data within them) by SCB to the SEC for the purposes of the Required Access Arrangements will be consistent with the requirements and restrictions of UK data protection law.

6. OTHER REQUIREMENTS NEEDING TO BE MET

- 6.1 SCB would also need to comply with a range of other requirements under the UK GDPR and UK DPA in order to disclose personal data to the SEC lawfully for the purposes of the Required Access Arrangements. We refer to these other requirements only briefly because, in our view, they do not place fundamental obstacles in the way of lawful disclosure.

- 6.2 These other requirements include:⁴⁸

⁴⁸ This is not intended as an exhaustive exposition of all relevant requirements of the UK GDPR and UK DPA, but to indicate the key requirements that may apply to SCB in respect of disclosures to the SEC for the purposes of the Required Access Arrangements.

- 6.2.1 ***Legitimate interests assessment:*** SCB will be required to conduct and document a "legitimate interests assessment", pursuant to article 6(1)(f) of the UK GDPR, in respect of each disclosure (or category of disclosures) to be made to the SEC in the context of the Required Access Arrangements, though which it demonstrates that it has appropriately balanced its and the SEC's legitimate interests in disclosure against the interests and fundamental rights and freedoms of the data subjects. Whilst this is not an explicit requirement of UK data protection law, it is implicitly required by articles 5(2) and 24(1) of the UK GDPR: article 5(2) requires SCB to "be able to demonstrate compliance with" article 5(1), which in turn requires SCB only to process personal data "lawfully" (i.e. in accordance with article 6(1)); and article 24(1) requires SCB to "*implement appropriate ... organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the UK GDPR as a whole, including article 6(1)]*". The ICO has published guidance on the conduct of legitimate interest assessments at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> and we assume that SCB will already have a process in place for the conduct of such assessments.
- 6.2.2 ***Data minimisation:*** SCB will be subject to a general "data minimisation" principle, under article 5(1)(c) of the UK GDPR, requiring it to ensure that the personal data that it discloses or otherwise processes are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. SCB should therefore seek to ensure that it does not disclose personal data to the SEC which fall outside the scope of the SEC's lawful requests, and should (as also discussed in paragraph 5.7.2(c)(iv)(B) above) consider in each case whether the SEC's requests for personal data are appropriately focussed on matters pertinent to the relevant subject matter, although acknowledging that it will ultimately be for the SEC to determine what personal data it needs.
- 6.2.3 ***Transparency:*** SCB will be obliged by articles 13 or 14 of the UK GDPR, subject to limited exceptions,⁴⁹ to provide information to data subjects about its processing of their personal data and related matters. This obligation will arise

⁴⁹ There are exceptions which may be relevant in some circumstances. For example, (i) in the case of personal data which SCB has not received directly from the data subject but from a third party source, an exception would apply (under article 14(5)(b) of the UK GDPR) if providing the required information to the data subject was impossible or would involve disproportionate effort; and (ii) SCB would be exempt under paragraph 2 of schedule 2 to the UK DPA from any obligation to inform data subjects of disclosure to the SEC (or other processing) of their personal data for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders if informing them would prejudice those purposes.

irrespective of any disclosure for the purposes of the Required Access Arrangements, by virtue of SCB's processing of the same personal data for other purposes, but it will include requirements to inform data subjects of the purposes for which the data are processed, the lawful basis for the processing (and the legitimate interests served, in the case of processing based on the legitimate interests condition) and the persons, or categories of person, to whom the data will be disclosed. SCB should therefore ensure that the privacy notices that it presumably routinely provides to its employees, client contacts and other data subjects appropriately address the possibility of disclosure for the purposes of the Required Access Arrangements.

- 6.2.4 ***Records of processing activities:*** SCB will be obliged by article 30 of the UK GDPR to maintain internal records of its processing of personal data. As with its transparency obligations, this obligation will arise irrespective of any disclosure or other processing for the purposes of the Required Access Arrangements, but SCB will need to ensure that its article 30 records cover disclosure and other processing for the purposes of those arrangements as well as SCB's other processing.
- 6.2.5 ***Technical and organisational security measures:*** SCB will be obliged by article 32 of the UK GDPR to have appropriate technical and organisational measures in place to protect the personal data that it controls. This requirement applies to all of SCB's personal data and doubtless SCB already has robust security measures in place. Although the Required Access Arrangements by their nature involve (authorised) disclosure of personal data, SCB should ensure that appropriate security measures are in place to protect disclosed personal data, while they remain within its control, through the process of disclosure to the SEC, so as to prevent interception and other forms of security breach.
- 6.2.6 ***Appropriate policy document:*** As discussed in paragraph 5.5.9(a)(iv) above, if the personal data to be disclosed include special category data or criminal offence data, SCB will be required by paragraphs 5 and 39 of DPA Schedule 1 to have a policy document in place governing its processing of special category data in the relevant category and/or of criminal offence data. This document will need to meet various requirements, set out in paragraph 39, and will need to be retained in accordance with paragraph 41.
- 6.2.7 ***Fee:*** As a controller of personal data, SCB will be obliged under the UK Data Protection (Charges and Information) Regulations 2018, which were made under the UK DPA, to pay a small annual fee, and provide some limited associated information, to the ICO. This obligation arises (although subject to

certain limited exceptions) irrespective of any need to disclose personal data to the SEC. Our understanding, based on the copy of the register of fee payers published by the ICO on its website, is that SCB has not paid the annual fee. Whilst we have not considered the point in detail, we think it unlikely that SCB's disclosures to the SEC would fall within the scope of any of the exceptions to the obligation to pay the fee. We therefore recommend that SCB should pay the fee.

- 6.2.8 **Accountability:** SCB will have various so-called "accountability" obligations under the UK GDPR, with some relevance to the Required Access Arrangements. We have, for example, already mentioned the need to conduct and document a legitimate interests assessment pursuant to article 6(1)(f) of the UK GDPR (as set out in 6.2.8 above) and to keep a written record of its assessment of the lawful basis on which disclosures are made. More broadly, SCB will be subject to a general obligation under article 24 of the UK GDPR to implement appropriate measures to ensure, and be able to demonstrate, compliance with the UK GDPR, which, given the nature of SCB's operations, will include a requirement to have appropriate policy, training, other communications and audit arrangements in place. If SCB has appointed a data protection officer under article 37 of the UK GDPR, it may in some circumstances be obliged to consult that officer about disclosures requested by the SEC. In some limited circumstances SCB may also be obliged, under article 35 of the UK GDPR, to conduct a formal data protection impact assessment of proposed disclosures to the SEC, although in practice this is unlikely unless SCB is required to disclose large quantities of special category data or criminal offence data.

7. CONFIDENTIALITY ISSUES

- 7.1 In the absence of express contractual confidentiality commitments (see paragraph 1.3 above), the English law of confidence will imply a duty of confidentiality into a contract wherever the relationship between the parties is such as to create a reasonable expectation of confidentiality. This will apply to SCB as a provider of financial services to its clients and as the employer of its employees. The duty of confidentiality can also arise in the context of other, non-contractual, relationships.
- 7.2 The duty of confidentiality is not absolute but, rather, will prohibit mis-use of information of a confidential information which SCB receives from, or otherwise acquires in the course of dealing with, a client or employee (or from another person, where the duty arises). In particular, it will prohibit *disclosure* of confidential information except in certain limited circumstances.

7.3 In particular:

- 7.3.1 SCB will in our view be entitled to disclose *employees'* confidential information, or the confidential information of other *individuals*, provided the disclosure does not breach the UK GDPR or UK DPA.
- 7.3.2 SCB will be entitled to disclose confidential information relating to (non-individual) *clients*, or other corporate persons to whom it may owe a duty of confidentiality, with their *consent*. Consent, for these purposes, need not meet the standards set by the UK GDPR (see paragraph 1 in part I of Annex A to this memorandum) – an express or implied consent, indicated by taking a positive step, to disclosure to the SEC, or of disclosures to a category of persons which includes the SEC, will be sufficient.
- 7.3.3 We assume that, in accordance with our experience of normal market practice, SCB will have obtained appropriate consents, allowing it to disclose confidential information to the SEC for the purposes of the Required Access Arrangements (or more generally) from all or substantially all of its clients and other relevant counterparties.
- 7.3.4 If SCB has *not* obtained consent from any given client or other relevant counterparty, SCB will still be entitled to disclose confidential information relating to that client or other counterparty "*where there is a duty to the public to disclose*".⁵⁰ In our view, this condition will be met in the circumstances in which the general public interest conditions discussed in paragraph 5 above are met: the test of being "*necessary for important reasons of public interest*"⁵¹ or "*necessary for reasons of substantial public interest*" is in our view the same test as the test of there being "*a duty to the public to disclose*".
- 7.3.5 In summary, we assume for the purposes of this memorandum that SCB will have obtained consents which are sufficient to allow it to disclose confidential information relating to its corporate clients and other counterparties for the purposes of the Required Access Arrangements. Where it has not obtained such consents, it will in our view be entitled to make those disclosures on the basis of a duty to the public to disclose, subject to the same limited considerations as are set out in paragraph 5.7.2(c)(iv), (d) and (f) above in relation to disclosures of personal data.

⁵⁰ The quote is from the judgment of Bank L.J. in the *Tournier* case (see footnote 12 on page 4, above), at 472.

⁵¹ See paragraph 5.6.7 above.

**C L I F F O R D
C H A N C E**

CLIFFORD CHANCE LLP

Yours sincerely,

Clifford Chance LLP

Clifford Chance LLP

Annex A – lawful bases for processing under UK GDPR article 6(1)

Part I – available lawful bases

The lawful bases available to justify processing of personal data under article 6(1) of the UK GDPR are as follows:

- "(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation⁵² to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;⁵³
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

⁵² Article 6(3) of the UK GDPR goes on to clarify that the reference to compliance with "law" is to compliance with *domestic (UK)* law.

⁵³ Article 6(3) goes on to clarify that, for this condition to apply, the basis for the processing must be laid down in *domestic (UK)* law.

Part II – brief discussion of the first six available lawful bases under article 6(1)

Consent

1. Our instructions invited us to consider the possibility of predicating our opinion on an assumption that necessary ***consents*** will have been obtained to permit SCB to disclose information as necessary for the purposes of the Required Access Arrangements. Whilst data subject consent is one of the lawful bases on which personal data can be processed, (under article 6(1)(a) of the UK GDPR), however, in our view it would be unrealistic to assume that SCB will have obtained effective data subject consents to allow it to make relevant disclosures of personal data to the SEC. The UK GDPR's conditions for an effective consent are very stringent. For a consent to be effective in these circumstances it would need to be genuinely voluntary – that is, the data subject would need to have been informed that their personal data might be disclosed to overseas regulatory authorities, and given the option of giving or withholding their consent in their absolute discretion, without suffering adverse consequences if they withheld their consent; taken a positive step to indicate their consent; and not subsequently withdrawn their consent (which they would be free to do in their absolute discretion). Effective consents from SCB employees would be particularly difficult to obtain, given the imbalance of power between employer and employee. We therefore assume that effective consents will generally ***not*** have been obtained.

Necessity for performance of a contract, to protect the data subject's vital interests or for the exercise of official authority vested in the controller

2. The lawful bases set out in articles 6(1)(b) (*necessity for performance of a contract*) and (d) (*necessity to protect the data subject's vital interests*), and the second of the lawful bases set out in article 6(1)(e) (*exercise of official authority vested in the controller*), are by their nature unlikely to apply to disclosure or other processing for the purposes of the Required Access Arrangements except, possibly (in some cases), in exceptional circumstances. We do not, therefore, consider them in this memorandum.

Necessity for the performance of a legal obligation

3. We note in Part I of this Annex that, by virtue of article 6(3) of the UK GDPR, the lawful basis in article 6(1)(c) (*necessity for performance of a legal obligation*) can only be relied upon based on an obligation under ***UK domestic law*** – any ***U.S.*** legal obligation to co-operate in the Required Access Arrangements does not, therefore, implicate this lawful basis.

As noted in the ICO Letter,⁵⁴ SCB, as a licensed firm for the purposes of UK financial services regulation, is under a UK domestic legal obligation to "*deal with its regulators [including overseas regulators such as the SEC] in an open and cooperative way*".⁵⁵ In our view, however, an obligation to deal with the SEC in an open and cooperative way will not amount to an obligation to disclose to the SEC all information that the SEC requests, in circumstances where the disclosure would be unlawful under English law in the absence of the obligation to cooperate, even where SCB is required by U.S. law or regulation to make the disclosure. SCB could in principle deal with the SEC in an open and cooperative manner for the purposes of its UK regulatory obligations while refusing to disclose some requested personal data to the SEC on UK data protection grounds, if other lawful bases do not justify the disclosure or it would breach article 9 or 10 or Chapter V of the UK GDPR. While *some* disclosures for the purposes of the Required Access Arrangements may be justified on this lawful basis, therefore, it will not in our view apply to *all* such disclosures. Similarly, as a bank, SCB is subject to the Prudential Regulatory Authority's Fundamental Rules that interpret references to "regulators" within FCA Principle 11 to include foreign regulators.⁵⁶

Necessity for the performance of a task carried out in the public interest

4. Article 6(1)(e) provides a lawful basis for processing personal data which is "*necessary for the performance of a task carried out in the public interest [or in the exercise of official authority] vested in the controller*". We note in Part I of this Annex that this basis for processing must be laid down in UK domestic law. In paragraph 5.7 in the body of this memorandum we discuss the question of whether cooperation in the Required Access Arrangements is in a public interest which is recognised in UK domestic law. Whilst the scope of article 6(1)(e) is not absolutely clear, however, in our view it is not sufficient for these purposes that the processing is carried out in a public interest which is recognised in UK domestic law. Rather, it must be carried out in furtherance of a public interest task which is allocated to SCB under UK domestic law.⁵⁷

⁵⁴ The ICO Letter does not, however, consider the question of whether a firm's obligations under Principle 11 of the FCA Handbook are sufficient to bring disclosures to the SEC within the scope of article 6(1)(c) of the UK GDPR.

⁵⁵ See Principle 11 of the FCA Handbook and related guidance PRIN 1.1.6(g).

⁵⁶ See <https://www.prarulebook.co.uk/rulebook/Content/Part/211136/04-10-2021>. Fundamental Rule 7 is the equivalent to FCA Principle 11. Rule 3.6 is the equivalent of PRIN 3.4.5R. The PRA does not have an equivalent to PRIN 1.1.6(g). PRIN 3.4.5R provides that references to "regulators" in Principle 11 include foreign regulators.

⁵⁷ The text of article 6(1)(e) is ambiguous in one respect – it is not clear on the face of the Regulation whether the words "*vested in the controller*" qualify the word "*task*" or only the words "*official authority*". We understand, however, that the German language text of article 6(1)(e) in the EU version of the GDPR, which is persuasive for the purposes of interpretation of the UK GDPR, clarifies that "*vested in the controller*" *does*

Mere cooperation with an overseas regulatory authority would not in our view amount to a task of this nature. Even disclosure to a UK regulatory authority, performing a task carried out in the public interest, would not fit within this lawful basis: SCB would either be obliged to co-operate by UK domestic law, in which case article 6(1)(c) of the UK GDPR would apply (pursuant to article 6(3) of the UK GDPR); or it would be co-operating voluntarily, in which case it would need to consider whether disclosure based on the legitimate interests lawful basis in article 6(1)(f) applied. The ICO's guidance on article 6(1)(e) is consistent with this analysis.⁵⁸

qualify the reference to a "*task*". For disclosure to the SEC to qualify as a "*task*" for the purposes of article 6(1)(e), therefore, it would need not only to be carried out in the public interest but also to be "*vested in SCB*", and, by virtue of article 6(3), this vesting would have to have a basis in UK domestic law.

We have considered the possibility that the ICO Letter might itself form a basis in UK domestic law for the vesting in SCB of a task comprising disclosure to the SEC in the context of the Required Access Arrangements. In our view, however, while the ICO Letter is "law" for the purposes of article 6, its mere identification and discussion of the role of the SEC under U.S. law and various data protection issues that might affect disclosures to the SEC by a UK firm cannot in our opinion be considered to vest any particular task in any given UK firm.

⁵⁸ The ICO's guidance is at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/>. Please note in particular the example given of retailers, co-operating with a UK public authority which is collecting personal data from them in pursuance of a public interest task vested in it. The ICO takes the view that the retailers themselves cannot rely on article 6(1)(e) because the relevant public interest task is not vested in them (instead, they would rely on the legitimate interests lawful basis in article 6(1)(f)).

Annex B – conditions for processing special category data under UK GDPR article 9(2)

Part I – conditions

The conditions one of which must be met to allow processing of special category data are as follows:

- "(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition ... may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to [certain] conditions and safeguards ...

- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of [domestic law] which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) [of the UK GDPR] (as supplemented by section 19 of the [UK DPA]) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

Part II – brief discussion of article 9(2) conditions that will not apply, or will only apply in exceptional circumstances

1. Regarding *consent* (article 9(2)(a)), see paragraph 1 of part II of Annex A to this memorandum. The same considerations apply to consent for the purposes of article 9(2)(a).
2. The conditions set out in articles 9(2)(b) (*UK domestic law employment, social security and social protection law rights and protections*), (c) (*vital interests of the data subject*), (d) (*non-profit bodies*), (e) (*data manifestly made public*), (h) (*preventative or occupational medicine*), (i) (*occupational health*) and (j) (*archiving*), are by their nature unlikely to apply to disclosure or other processing for the purposes of the Required Access Arrangements except, possibly (in some cases), in exceptional circumstances. We do not, therefore, consider them in this memorandum. The same applies to the second limb of the condition set out in article 9(2)(f) (*necessity where courts are acting in their judicial capacity*).
3. The first limb of the condition set out in article 9(2)(f) (*necessity for the establishment, exercise or defence of legal claims*) is the same in scope as the condition allowing processing of criminal offence data in paragraph 33(c) of Part C of DPA Schedule 1 – see our brief discussion of that condition in footnote 19 on page 2 of this memorandum.

Annex C – article 49 derogations from the UK GDPR international personal data transfer restrictions

Part I – derogations

The derogations allowing transfer of personal data to a country or territory outside the UK which is not determined to ensure adequate protection for personal data, where appropriate safeguards are not in place to protect the transferred data, are as follows:

- "(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;⁵⁹
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to domestic law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by domestic law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in article 45 or 46 [regarding appropriate safeguards], and none of the derogations for a specific situation [in (a) to (g)] is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the

⁵⁹ Article 49(4) goes on to provide that the public interest relied upon must be recognised in UK domestic law.

circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the [ICO] of the transfer. The controller shall, in addition to providing the information [otherwise required to be provided under the UK GDPR], inform the data subject of the transfer and on the compelling legitimate interests pursued."

Part II – brief discussion of article 49 derogations that will not apply, or only in exceptional circumstances

1. Regarding *consent* (article 49(1)(a)), see paragraph 1 of part II of Annex A to this memorandum. The same considerations apply to consent for the purposes of article 49(1)(a).
2. The derogations set out in articles 49(1)(b)/(c) (*performance of a contract*), (f) (*vital interests of the data subject*) and (g) (*published register*), are by their nature unlikely to apply to disclosure or other processing for the purposes of the Required Access Arrangements except, possibly (in some cases), in exceptional circumstances. We do not, therefore, consider them in this memorandum.
3. Regarding the derogation set out in article 49(1)(e) (*necessity for the establishment, exercise or defence of legal claims*), again see our brief discussion of the equivalent condition in paragraph 33(c) of Part C of DPA Schedule 1 in footnote 19 on page 2 of this memorandum.
4. The derogation in the second un-numbered sub-paragraph of article 49(1) (*compelling legitimate grounds for non-repetitive transfers*) is included for reliance only in exceptional circumstances, where it is necessary to rely on a derogation but none of the specific derogations (a) to (g) applies. It is unlikely, in our view, that SCB would be able to rely on it other than exceptional circumstances – we note, in particular, that it would require SCB to provide "*suitable safeguards*" to protect the transferred personal data, and also to notify both the ICO and the data subjects of the transfer – in our view, this would require specific notification to each data subject of the particular contemplated transfer, which would presumably be impracticable in many circumstances. We are not aware of this derogation being relied upon in practice, and it would categorically not be available if a given transfer was "*repetitive*" (i.e. there had been or would be other similar transfers) or it involved transfer of personal data relating to more than "*a limited number*" of data subjects. We have not identified circumstances in which SCB would have a lawful basis for disclosure under article 6(1), would not be able to rely on article 49(1)(d) and could instead rely on this derogation. That being the case it is in our view not relevant for the purposes of the Required Access Arrangements.