Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Raquel Fox
Director
Office of International Affairs
U.S. Securities and Exchange Commission
202-551-3403

By email only: [redacted]

11 September 2020

Dear Raquel Fox,

RE: Securities and Exchange Commission transfer analysis.

Thank you for the information you have supplied in seeking understanding of the application of GDPR provisions as they apply to UK based firms seeking to comply with their regulatory obligations to yourselves.

The Information Commissioner has been asked to provide a view as to the application of and regulation of international transfers as they apply to certain United Kingdom (UK) based companies with United States (US) regulatory obligations, in particular under Chapter V GDPR *Transfers of personal data to third countries of international organisations*.

I should point out that the Commissioner reserves the right to make changes or form a different view based on further findings or changes in circumstances. The Commissioner's view, set out in this letter, is consistent with the European Data Protection Board guide lines, but is provided for the legal context of UK firms only and should not be regarded as pan EU advice.

Background

We understand that, under US law, certain firms must retain certain books and records, and must gather or generate, keep secure and process information, documents and materials, and must provide these directly to the US Securities and Exchange Commission (SEC) and make them available for inspection upon SEC staff's request.

These firms include UK domiciled firms or branches that are registered, required to be

registered or otherwise regulated by the SEC as investment advisers (IAs), investment managers or investment companies, brokers or dealers (BDs), credit rating agencies, transfer agents, clearing agencies, exchanges and other trading venues, trade repositories, security based swap dealers and major security-based swap participants, and other market participants. These firms also include UK issuers that have equity securities or depositary receipts (DRs) registered with the SEC under the US Securities Act of 1933 and the US Securities Exchange Act of 1934 that are listed on a US exchange or market (together "SEC regulated UK firms"). The SEC regulated UK firms may or may not be subject to the oversight of the FCA, Bank of England, or another UK financial regulatory authority.

SEC staff requests these books, records and other materials to evaluate compliance with legal obligations designed to ensure the proper legal administration of SEC regulated UK firms and to prevent and/or enforce against potential illegal behaviour such as money laundering, fraud or sanction evasion.

The SEC is legally entitled to request and examine such books and records which may involve sources of information such as e-mails sent or received by staff (internally and externally with prospects and clients), as well as meeting notes and other written materials prepared by an SEC regulated UK firm's employees. The SEC has the power and authority to require the production of books and records on demand directly to the SEC.

In an examination, SEC staff will send the SEC regulated UK firm a document request that requires that firm to provide certain enumerated information. Failure to generate and keep such books and records would violate the firm's regulatory requirements. Failure to provide information as requested would also generally violate the firm's regulatory requirements, would be deemed to be impeding an examination, and might result in an enforcement referral or, if severe, an enforcement action.

You have informed us that the requested information for examination focusses on a wide range of information, including office policies, procedures, organisation structures, staff lists, director details (publicly available in the UK), employee disciplinary history, employment applications/questionnaires, employee personal trading records, financial transaction records, customer complaints, customer agreements, internal communications, and documents relating to service providers such as consultants and auditors. In addition, you have informed us that it is the SEC's practice to limit the type and amount of personal data it requests during examinations to targeted requests based on risk and related to specific clients and accounts, and employees. The requested information may include some limited criminal records data and 'special category data' under the GDPR.

SEC examinations are non-public. Information, data and documents received by the SEC are maintained in a secure manner and, under strict US laws of confidentiality, information about individuals cannot be onward shared save for certain uses publicly disclosed by the SEC, including in 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. Information from SEC examinations is also subject to the US Freedom of Information Act controls that protect confidential information. The SEC uses what it obtains solely for its own lawful, regulatory purpose. It is itself subject to audit by the US Government Accountability Office and other governmental oversight.

GDPR compliance

The transfers of data from the SEC regulated UK firms to the SEC contain personal data, and therefore those firms will need to comply with the rules on international transfers set out in Chapter V of the GDPR.

The general principle for international transfers under GDPR is that personal data which is transferred to third countries continues to be protected by appropriate safeguards. Article 44 of GDPR provides that *'All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.*

As is clear from the GDPR text, the GDPR is not a barrier to international transfers. It provides a range of transfer tools and gateways, seeking to ensure that data retains the same level of data protection when it travels outside of the EU. This key principle was confirmed by the CJEU in the recent *Schrems II* case. Those safeguards can either be provided by law in the third country (i.e. there is an adequacy decision in place) or if one of the transfer tools is put in place (laid out in Article 46 of the GDPR).

The GDPR also recognises that there are circumstances when, balancing data protection and privacy rights against other human rights, it is necessary and proportionate for a transfer to take place without such protection; these are set out in the Art 49 derogations. The GDPR envisages that transfers will be required from time to time when Art 45 and Art 46 protections are not available, on the basis of the Art 49 derogations, such as consent, for the performance of a contract or where there is public interest.

As explained in the European Data Protection Board (EDPB)'s guidelines on Art 49, the derogations must be interpreted carefully so that the exception does not become the rule. In practice, this means that the derogations should not be relied on for making transfers "on a large scale and in a systematic manner". Their use must be considered on a case by case basis, with careful thought and analysis, as the need for individual transfers arise. Records should be kept by firms making those transfers, to demonstrate their considerations.

ICO expectations in the regulatory context

In these circumstances, the ICO only has oversight of the SEC regulated UK firms sending information to the SEC. It has no extra-territorial oversight of the SEC and the

GDPR does not impose personal liability on SEC staff.

The Commissioner would expect the UK firms and SEC to work together to try and put in place an Article 46 transfer tool as a long term solution, if that is possible; the Commissioner will also be on hand to provide guidance on this, and is willing to engage with the UK government if necessary.

The Commissioner considers that there are circumstances when it is appropriate that information is transferred using the Art 49 derogations, in particular while an Article 46 transfer tool is put in place and where an Article 46 transfer tool is not possible. These derogations should be used on a case by case basis with the appropriate thought taken and recorded by the companies concerned.

Application of Art 49.1(d) the transfer is necessary for important reasons of public interest

In the circumstances outlined in the "Background" section, our view is that it is possible for SEC regulated UK firms to transfer personal information to SEC on the basis of the derogation set out in Art 49.1(d) – the transfer is necessary for important reasons of public interest.

There are three key areas we have considered:

1. We consider there are important reasons of public interest embedded in UK law (as required by Art 49.3)

We have explored with you and the Financial Conduct Authority (FCA) the UK public interest which arises in your regulation of SEC regulated UK firms, including your requests for information which is a core part of that regulation. It is apparent that there are a number of overlapping lines of public interest, which are recognised in UK law, including:

- The UK is signatory to the Financial Stability Board (FSB), which is comprised of the financial authorities from the G20 jurisdictions and non-G20 countries with large financial sectors, international financial institutions (such as the IMF), and international standard setting bodies. HM Treasury is a member of the FSB, alongside the Bank of England and Financial Conduct Authority, and has a seat on the FSB's Plenary and Steering Committee (the major decision making committee).

  The FSB has a 'Compendium of Standards', which lists the various economic and financial standards that are internationally accepted as important for sound, stable and well-functioning financial systems.

  The compendium includes (as one of its key standards) the International Organisation of Securities Commissions (IOSCO) 'Objectives and Principles of

Securities Regulations'. These IOSCO Objectives and Principles are consistent with SEC's and FCA's rules and regulations, including those on examinations.

As a key standard, the FSB has recognised that the IOSCO Objectives and Principles are materially relevant for fostering sound financial systems.

- Compliance with SEC rules by SEC regulated UK firms: (i) helps to prevent UK financial crimes from being committed; and (ii) helps to prevent the commission in the US of conduct that would amount to a UK financial crime.

> *The FCA has a regulatory objective to protect and enhance the integrity of the UK financial system: The Financial Services and Markets Act 2000 (FSMA) section 1D. This objective includes the UK financial system not being used for a purpose connected with financial crime: section 1D(2)(b). "Financial crime" includes acts or omissions that would have been an offence if they had taken place in the UK (section 1H(4)). The "UK financial system" means the financial system operating in the UK (section 1I). The combined effect of these provisions is that FSMA demonstrates that there is a UK public interest in UK-based firms not being used for the purposes of conduct* ***overseas*** *that would constitute a financial crime* ***if committed in the UK****.*

- For those SEC regulated UK firms which are also regulated by the FCA, the FCA Handbook requires (by law) those firms to "deal with its regulators in an open and cooperative way…" (Principle 11). The FCA explains in its guidance (PRIN 1.1.6G) that this includes overseas regulators:

> *Principle 11 (Relations with regulators) applies to world-wide activities; in considering whether to take regulatory action under Principle 11 in relation to cooperation with an overseas regulator, the FCA will have regard to the extent of, and limits to, the duties owed by the firm or other person to that regulator.*

2. Following the EDPB guidelines, the test which should be applied is that the transfer one of "strict necessity" for important reasons of public interest.

This means the sender of the data must pay particular attention to the necessity principle in the context of interpreting the 'public interest' derogation, and look to be see if there are "precise and particularly solid justifications"[1].

[1] *R (ota Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin). §36. This case was considering a 'strict necessity' test under the Law Enforcement Directive, which is analogous to this situation.

In practice this means that it is important to be able to identify the exact basis in EU or UK law for the relevant public interest (for example, as we have set out above), and carefully and precisely apply the 'necessary and proportionate' test.

As the ICO must interpret the GDPR in the light of the EU Charter of Fundamental Rights and the European Convention of Human Rights, a test of necessity or strict necessity must also incorporate proportionality, finding the balance between competing human rights.

3. We consider that the SEC requests outlined above would be strictly necessary and proportionate, taking the following into account:

- Just as for requests from any UK regulator, SEC regulated UK firms must be duly satisfied that your requests are within the scope of your regulatory powers and requirements, and keep a record of their considerations so they are able to evidence this, as part of a fully auditable governance process.

- Following EDPB guidelines, those requests for information should not be large scale and systematic. We understand that SEC requests are never regular and predictable, albeit the very largest SEC regulated UK firms may receive more requests.

Other GDPR obligations:

SEC regulated UK firms should of course also be complying with their other GDPR obligations. For example, they will need a lawful basis in Art 6 and a further processing condition for any special category data or criminal records data (set out in Art 9 and 10). The firms must also comply with their transparency obligations, they should be providing their customers and staff with privacy notices setting out how they will be handling their personal data, including potential transfers to the SEC. Further, to comply with the accountability principle, they should be keeping records of their processing of personal data including relevant decisions about international transfers.

Our approach to complaints:

Should an individual complain to the ICO about his/her data being transferred to the SEC without any appropriate safeguards in place, we would typically contact the SEC regulated UK firm to ask for their comments on the complaint.

We would not find there to be a breach of the GDPR transfer rules if the firm provided evidence that it had carefully considered and appropriately applied the Art 49.1(d) 'public interest' derogation.

Nevertheless, should there be a breach of GDPR by the SEC regulated UK firm, we would

take a proportionate and pragmatic approach in deciding whether to take enforcement action, acting in line with our Regulatory Action Policy[2].

The UK has left the European Union and is currently in a transition period when EU laws, including GDPR, continue to apply. At the end of this transition period on 1 January 2021 the UK GDPR will apply, which will contain very similar provisions. We do not anticipate any significant change to our approach to the application of the UK GDPR to the transfers of personal data by SEC regulated UK firms to you.

Conclusion

We welcome your willingness to discuss the potential for putting in place one of the Article 46 safeguards, which we recognize will take time.

Our view is that SEC regulated UK firms will be able to rely on the Art 49.1(d) 'public interest' derogation (on the basis set out in this letter) and we will explore whether an Art 46 transfer tool is appropriate. If it transpires that it is not possible to put in place an Art 46 transfer tool, the SEC regulated UK firms will be able to continue to rely on Art 49.1(d) 'public interest' derogation, on the same basis.

Yours sincerely,

[redacted]

James Dipple-Johnstone
Deputy Commissioner (Chief Regulatory Officer)

[2] https://ico.org.uk/media/about-the- ico/documents/2259467/regulatory-action-policy.pdf