Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

U.K. Privacy Regulator Clarifies How U.K. Firms May Respond to SEC Document and Records Requests

January 25, 2021

Key Points

- The United States Securities and Exchange Commission (SEC) is able to make requests of U.K. firms (including U.K. branches of non-U.K. firms) to provide books and records and other documents of SEC regulated entities, such as investment advisers and broker-dealers, as well as companies with U.S. securities that maintain a U.K. presence. The requested records and documents can often contain personal data subject to the U.K. General Data Protection Regulation (U.K. GDPR), which is in force in the United Kingdom post-Brexit and is currently materially the same as the European Union General Data Protection Regulation (EU GDPR).[1]
- In response to a request from the SEC, the U.K. Information Commissioner's Officer, U.K.'s data protection regulator (ICO), has published its letter to the SEC setting out the ICO's views on regulating relevant transfers of personal data, which will assist firms to understand how they can comply with both their SEC obligations and the U.K. GDPR.[2]
- In summary, a U.K. firm is likely to be able to provide the requested books and records and other documents containing personal data in reliance on the "public interest" derogation in Article 49(1)(d) U.K. GDPR, but firms will still have to consider whether the transfer is "necessary and proportionate", provide the appropriate disclosures to customers and staff and document their decision making process.
- This is a welcome clarification and provides U.K. firms with some comfort if they wanted to consider relying on the "public interest" derogation in complying with an SEC-initiated request for books and records and other documents, instead of or in addition to other derogations, such as explicit consent under Article 49(1)(a) and establishment, exercise or defense of legal claims under Article 49(1)(e).
- Against this backdrop, we understand that the SEC has ended its moratorium on the registration of U.K. managers and once again permits registration.

Introduction

Contact Information
If you have any questions concerning this alert, please contact:

Peter I. Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Helen Marshal
Partner
helen.marshall@akingump.com
London
+44 20.7661.5378

Michael A. Asaro
Partner
masaro@akingump.com
New York
+1 212,872.8100

Jason M. Daniel
Partner
jdaniel@akingump.com
Dallas
+1 214.969.4209

Barbara Niederkofler
Partner
bniederkofler@akingump.com
New York
+1 212.872.8149

Ezra Zahabi
Partner
ezra.zahabi@akingump.com
London
+44 20.7661.5367

Jenny Arlington
Counsel
jarlington@akingump.com
Counsel
+44 20.7661.5367

Regulated firms are often required by their regulators to provide certain records and documents. These records and documents can often contain personal data, which is very broadly defined under the U.K. GDPR, and includes a mere name, or work email, or other contact details, as well as more sensitive information such as health data.

In the U.K., the cross-border transfer and disclosure of personal data is governed by the U.K. GDPR, and the starting position is that such transfers are restricted. Under Article 44 U.K. GDPR, personal data can only be transferred to a "third country" (i.e., outside the U.K.) if it is done so in accordance with one of the lawful mechanisms set out in Chapter V of the U.K. GDPR. The rationale behind these restrictions is that the protection guaranteed under the U.K. GDPR to personal data of U.K. individuals should "travel" with the data, and so if the data leaves the U.K., it should not lose those protections.

It appears that the SEC has requested guidance from the ICO on the ICO's view regarding the applicability and regulation of certain transfers of personal data to the SEC. On January 19, 2021, the SEC alerted the public that the ICO published its response to the SEC, which is dated September 11, 2020 (i.e., during the Brexit Transition Period when European Union (EU) laws continued to apply). The Brexit Transition Period ended on December 31, 2020, but the ICO noted in its letter that it did "not anticipate any significant change to [its] approach".

It is worth noting that in relation to transfers of personal data to the SEC, two of the lawful mechanisms are not available:

- There is no "adequacy decision", which would designate the U.S. as a country which provides adequate protection of personal data, and hence would permit transfer to the United States: see Article 45 U.K. GDPR. This is in contrast to transfers to regulators in EU jurisdictions, for example, as the U.K. has temporarily deemed the EU member states, Iceland, Liechtenstein, Norway and Switzerland to be adequate on a transitional basis (see further detaills here).
- There are no "appropriate safeguards" in place between U.K. firms as exporters of the personal data, and the SEC as importer of the data, within the meaning of Article 46 U.K. GDPR, which would permit such transfers. The ICO noted that it "would expect … UK firms and [the] SEC to work together to put in place" adequate safeguards as a "long term solution". However, the ICO expressly referred to Schrems II, the judgment of the Court of Justice of the EU dated July 2020, which significantly impacted the validity and availability of some such safeguards, including standard contractual clauses and binding corporate rules (see further details here). In that context, the ICO stated that it could be explored if an Article 46 transfer tool is "appropriate", or indeed "possible"; and that putting such a mechanism in place, "if that is possible", "will take time".

  In light of the above, the ICO clarified that the derogation in Article 49(1)(d) U.K. GDPR could be relied upon.

Article 49(1)(d) Derogation

The ICO's analysis states that U.K. firms should generally be able to rely on the derogation in Article 49(1)(d) U.K. GDPR, which allows transfers that are "necessary for important reasons of public interest".

The ICO considered that complying with SEC document requests could be considered within the "public interest" of the U.K. and justified this determination by reference to the following factors:

- The U.K. is a signatory to the Financial Stability Board (FSB), which has adopted the International Organisation of Securities Commissions' (IOSCO) "Objectives and Principles of Securities Regulations". The ICO determined that these Objectives and Principles were consistent with the SEC and the U.K. Financial Conduct Authority's (FCA) rules and regulations surrounding examinations.
- Compliance with the SEC rules by U.K. firms (i) helps to prevent U.K. financial crimes and (ii) helps to prevent actions in the U.S. which would amount to crimes in the U.K. if performed in the U.K. (so-called 'double criminality').
- Principle 11 of the FCA's Principles for Businesses requires a U.K. firm to "deal with its regulators in an open and cooperative way", which includes non-U.K. regulators.[3]

The ICO then recognized that reliance on the "public interest" derogation also required that any transfer be "strictly necessary" and "proportionate", as required under Article 49(1)(d) U.K. GDPR and the underlying principles of data minimization, fairness and purpose limitation. While each U.K. firm will have to satisfy itself that these tests are met in each particular case, the ICO has indicated that it thought the tests could be met in the cases raised by the SEC in its request for ICO's view, including where the SEC had submitted that:

- It was 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".
- "SEC examinations are non-public" and "[i]nformation, data and documents received by the SEC are maintained in a secure manner and, under strict U.S. laws of confidentiality, information about individuals cannot be onward shared save for certain uses publicly disclosed by the SEC".

As a result, the ICO indicated that if there were to be a complaint against a firm on the grounds that it provided documents to the SEC in response to an examination, the ICO "would not find there to be a breach of the [U.K. GDPR] transfer rules if the firm provided evidence that it had carefully considered and appropriately applied the [Article 49(1)(d)] 'public interest' derogation". The ICO confirmed that it would take a proportionate and pragmatic approach in deciding whether to take enforcement action, reiterating similar guidance regarding its approach (see details here).

SEC Response

Prior to this analysis from the ICO, the SEC had been concerned that U.K. firms might not lawfully be able to respond to SEC requests for books and records and other documentation in accordance with U.K. GDPR. As such, there had been in place an SEC moratorium on the registration of U.K. firms.

Following this ICO analysis, however, and particularly the clarification that firms can look to the "public interest" derogation to respond to SEC requests, we understand that the SEC has ended its moratorium on the registration of U.K. managers, and once again permits registration.

What Firms Should Do

If a U.K. firm (or a U.K. branch) receives a request for documents from the SEC which includes, or may include, personal data within the definition of the U.K. GDPR, it should consider the following questions, and document its determination as to each, in order to rely on the "public interest" derogation under Article 49(1)(e):

- Does the SEC's request appear to be proper and within the SEC's lawful authority?
- In light of the ICO's analysis in its letter to the SEC, does the "public interest" derogation apply? This would require carrying out an analysis of the exact basis in U.K. law for the relevant public interest.
- Given the nature of the personal information which has been requested, is it "necessary and proportionate" for that data to be provided, particularly considering if any special categories of data (e.g. health data) or criminal records data has been requested?

In addition, U.K. firms should consider their other obligations under the U.K. GDPR in this context, including the requirement in the first instance to have a lawful basis for the underlying processing of personal data; the necessity to provide adequate notice to its customers and staff of the processing, transfer and disclosure of data to the SEC; and the obligation to keep records of their processing activities in order to be able to demonstrate compliance with the U.K. GDPR.

It should also be noted that in cases where the "public interest" derogation cannot lawfully be relied upon, other derogations may still be available to U.K. firms, such as relying on explicit consent or transfers and disclosure for the establishment, exercise or defense of legal claims.

As well as data protection considerations, we also note that U.K. firms regulated by the FCA or the Prudential Regulatory Authority (PRA) should also consider whether receiving a document or record request from the SEC (or any other international regulator) might trigger a requirement to make a notification to the FCA or the PRA accordingly.

[1] U.K. GDPR is the version of the European Union General Data Protection Regulation (EU GDPR) which was incorporated into U.K. law at the end of the Brexit Transition Period under the European Union (Withdrawal) Act 2018 ("EUWA 2018"). U.K. GDPR is in very similar terms to EU GDPR, with some amendments made through "Exit Regulations" issued under section 8 EUWA 2018.

[2] https://ico.org.uk/media/2619110/sec-letter-20200911.pdf. Notably, then-Acting SEC Chairman Elad L. Roisman released a statement in connection with the ICO's release, calling it a "welcome development demonstrating that securities regulatory oversight frameworks can coexist with robust data protection standards." https://www.sec.gov/news/public-statement/roisman-uk-ico-personal-data-transfers-data-sec.

[3] See PRIN 1.1.6 G: https://www.handbook.fca.org.uk/handbook/PRIN/1/1.html.

akingump.com