Proskauer

New Focus and Compliance Approach Needed for Privacy and Cybersecurity

The Capital Commitment Blog on **April 8, 2021**

In 2020, we saw an increased regulatory focus on cybersecurity. Though former SEC Chairman Clayton largely took the view that existing statutes and regulations were sufficient, the Division of Examinations increased exam activities in the space while agencies like FinCEN increased enforcement against violators. We can expect to see a continued focus on cybersecurity going forward, but it is unclear seen whether it will remain among the top priorities of the SEC. As set forth in Risk #1, we believe that the presumptive Chairman, Gary Gensler, will take a more active approach generally and, as part of that, we expect a heightened focus on cybersecurity. Sponsors are a theoretically high value target for attack because even relatively small sponsors often control billions of dollars (whether directly or indirectly) and have highly confidential information concerning their investors and partners. It is important that sponsors' commitment to, and investment in, cybersecurity systems, policies, and procedures is commensurate with their risks and profile in fact. State voters have also increased their focus on cybersecurity and privacy. The California Consumer Privacy Act of 2018 ("CCPA") became operative on January 1, 2020, requiring qualifying businesses to enable consumers to know about and control the information collected about them. In November 2020, California voters passed the California Privacy Rights Act of 2020 ("CPRA") in an effort both to expand and strengthen the scope of the CCPA. (The CPRA will become operative on January 1, 2023.) Because both the CCPA and CPRA define consumers and businesses broadly, private investment funds and their sponsors and managers may be considered "qualifying businesses" and information they collect and use about their employees, job applicants, investors, and prospective investors (including KYC information) residing in California could be subject to either or both of the acts.

Overseas, now that the UK has left the EU, funds that operate in London and across the EU bloc must use a suitable route for the transfer of personal data. Thankfully, on February 19, 2021, the European Commission published a draft decision that the UK has an adequate level of protection for personal data (the UK has already made the reciprocal determination and has adopted the EU's General Data Protection Regulation (GDPR) into national law). The next step is for the draft adequacy decision to be approved by the Member States.

Funds with data flows the EU/UK and between the US lost the protection of the EU-US Privacy Shield in mid-2020 so they will need to use one of the appropriate safeguards to transfer personal data – e.g., standard contractual clauses (SCCs) (for intragroup or third party transfers) or binding corporate rules (for intragroup transfers) – or else rely upon one of the applicable derogations. Funds must also have "appropriate supplementary measures" in place so that personal data transferred outside of the EU/UK is protected in any third country to the same extent as it would be under the GDPR.

Areas to watch in 2021 include possible divergence between interpretation of UK-GDPR and EU-GDPR, updates to SCCs that may require funds to replace existing clauses, and further guidance on appropriate supplementary measures.

Read more of our Top Ten Regulatory and Litigation Risks for Private Funds in 2021.

Related Professionals

- **Margaret A. Dale**
  Partner
- **Mike Hackett**
  Partner
- **Timothy W. Mungovan**
  Chairman of the Firm
- **Dorothy Murray**
  Partner
- **Joshua M. Newville**
  Partner
- **Todd J. Ohlms**

Partner

- **Seetha Ramachandran**
  Partner
- **Ana Vermal**
  Partner
- **Jonathan M. Weiss**
  Partner
- **Kelly M. McMullon**
  Special International Labor, Employment & Data Protection Counsel
- **James Anderson**
  Senior Counsel
- **William D. Dalsen**
  Senior Counsel
- **Adam L. Deming**
  Associate
- **Hena M. Vora**
  Associate