



August 2018

Follow @Paul\_Hastings



## *Applying GDPR to Private Investment Funds: When to Ask an Expert*

By [Sarah Pearce](#) & [Max Rosenberg](#)

On May 25, 2018, the European Union's new data privacy regime took effect after a four year legislative development period. The General Data Protection Regulation ("GDPR") is now directly applicable in each EU member state and is designed to harmonize EU data protection rules.

Based on the broad scope of the GDPR, even non-EU private investment funds could be affected by the GDPR if they are being marketed in the EU.

While the fundamental principles of the EU's prior data protection regulations remain the same, there are significant changes effected by the GDPR and some of the new requirements will take time to implement. The penalties for non-compliance can be substantial—statutory fines for non-compliance can be up to 4% of annual gross revenue or €20 million (whichever is greater).

### **Scope**

The GDPR defines "personal data" as "information relating to an identified or identifiable natural person." This is significantly broader than the U.S. definition of personal data and in a private investment fund context this is likely to include: (i) data relating to a natural-person investor's identity (e.g., name, address, driver's license, phone numbers, email address, social security number, bank account detail); (ii) identity data relating to the private fund's directors or other employees; and (iii) data relating to business contacts.

The prior EU data protection regime applied to data controllers that are established in the EU and process personal data in the context of the data controller's activities or use equipment situated in the EU to process personal data.

However, the GDPR has extended the reach of EU data protection law such that non-EU organizations (such as non-EU private investment funds and their sponsors) will fall within its scope if they process the personal data of individuals in the EU in connection with goods or services offered to such individuals, or monitor the behavior of individuals within the EU.

### **Principal Application to Private Investment Funds and Their Sponsors**

Clearly private investments funds and their sponsors with offices in the EU or that are doing business in the EU and collecting and processing personal data of EU persons (such as EU-based employees and/or counterparties) will likely come within the scope of the GDPR.



In addition, the broad scope of the GDPR means that a private investment fund that is being marketed to natural persons in the EU with a view to accepting subscriptions from those individuals is likely to be caught by the GDPR—even if the private investment fund and its sponsor are not based in the EU.

However, non-EU private investment funds that only market to and accept subscriptions from EU institutions (e.g., sovereign wealth funds, pension funds, insurance companies) may not be subject to the GDPR. These investment funds and their sponsors may inadvertently acquire personal data about natural persons such as directors, officers, and other authorized representatives of the EU institution (e.g., authorized signatories and reporting contact persons), but may not be viewed as processing the personal data of these natural persons in connection with providing investment management and related services to the applicable EU institution.

While private investment funds are not generally considered to be high-risk businesses with regard to data protection compliance, a significant amount of personal data will be processed during the life cycle of a fund. In light of the potentially significant sanctions for non-compliance and the extra-territorial reach of the new rules, the data processing by private investment funds and their sponsors now merits expert analysis.

GDPR, if applicable, will require substantial changes to processes and procedures. There is no “one size fits all” for private investment funds, each structure is different and fairly granular data mapping exercises should be undertaken to fully understand the role and obligations of each fund-related party and their service providers in the processing of personal data. This will provide a useful starting point for establishing a clearly defined compliance program.



*If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:*

**London**

Sarah Pearce  
44.020.3023.5168  
[sarahpearce@paulhastings.com](mailto:sarahpearce@paulhastings.com)

**New York**

Lawrence J. Hass  
1.212.318.6401  
[larryhass@paulhastings.com](mailto:larryhass@paulhastings.com)

**Washington, D.C.**

Behnam Dayanim  
1.202.551.1737  
[bdyanim@paulhastings.com](mailto:bdyanim@paulhastings.com)

Max J. Rosenberg  
1.212.318.6229  
[maxrosenberg@paulhastings.com](mailto:maxrosenberg@paulhastings.com)

---

Paul Hastings LLP

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2018 Paul Hastings LLP.