The HEDGE FUND LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation

www.hflawreport.com Vol. 11, No. 24 June 14, 2018

PRIVACY

How the GDPR Will Affect Private Funds' Use of Alternative Data

By Robin L. Barton, *The Hedge Fund Law Report*

The E.U.'s General Data Protection Regulation (GDPR), which took effect May 25, 2018, primarily affects investment managers and private funds that are based in the E.U. The GDPR's restrictions on the processing of "personal data"[1] of individuals in the E.U., however, may affect managers and funds that are located outside the E.U. if they process the data of individuals located in the E.U. in connection with the offering of services to those individuals.

Because more funds are using alternative data in their operations – notably in driving their trading strategies and making investment decisions – the GDPR may impact how these funds obtain and use alternative data if that data contains what is arguably considered the personal data of individuals in the E.U.

To help readers understand the potential impact of the GDPR on funds' use of alternative data, The Hedge Fund Law Report interviewed Peter D. Greene, partner and vice-chair of the investment management group at Lowenstein Sandler. This article presents his insights.

For more from Greene, see our three-part series on the opportunities and risks presented by big data: "Acquisition and Proper Use" (Jan. 11, 2018); "MNPI, Web Scraping and Data Quality" (Jan. 18, 2018); and "Privacy Concerns, Third Parties and Drones" (Jan. 25, 2018).

HFLR: Can you explain what impact the GDPR will have, in general, on private funds?

Greene: Some of the basic steps fund managers need to take right now for GDPR-compliance purposes include understanding all of the different ways they use and share personal data; adding a GDPR addendum (or compliant covenants) to service agreements with any vendors that touch the data of the manager's E.U. employees or E.U. investors, or that provide alternative data that includes the personal data of E.U. residents; and updating their privacy policies and subscription agreements.

[See our two-part series "What Are the GDPR's Implications for Alternative Investment Managers?": Part One (Apr. 26, 2018); and Part Two (May 10, 2018).]

HFLR: More specifically, how will the GDPR affect how private funds buy and use alternative data?

Greene: This is an important question for fund managers that consume data. As we know, more and more managers are starting to consume data, such as credit card panel data, social media data, app usage data and location intelligence data, to name a few. If a manager buys data, it may come into possession of what the E.U. regulators define as "personal data," which is different and broader than the U.S. definition of "personally identifiable information" (PII). In the E.U., a key question is whether a person can be identified on the basis of the data – essentially, can you reverse-engineer the data or combine it with other data you have access to in order to identify an individual? In the U.S., PII is more limited to categories such as name, Social Security number, address, etc.

Given the broader E.U. definition of personal data, whenever a fund manager is buying data from a vendor, it must obtain additional representations from the vendor regarding the GDPR. The manager will want assurances from the vendor that it is not receiving anything that constitutes personal data under the GDPR or, if it is receiving personal data, that the vendor is GDPR-compliant.

It remains to be seen whether managers will shy away from buying data that potentially includes the personal data of individuals in the E.U. For example, will managers stick to only U.S.-based credit card panel data? If so, that may mean that they will have a smaller universe of data. It may also make it more difficult to trade on a data basis in E.U.-listed companies (although certainly U.S.-based companies have E.U. customers). I am sure that managers that are comprehensive in their approaches to research and data have been buying E.U. customer data in order to evaluate U.S.-based companies, even though that E.U. data may be just a small slice of the overall revenue for that company.

The HEDGE FUND LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Vol. 11, No. 24 June 14, 2018

[See "Tips and Warnings for Navigating the Big Data Minefield" (Jul. 13, 2017).]

HFLR: What if a fund is generating or gathering alternative data internally, such as through web scraping? What impact may the GDPR have on those activities?

Greene: Right now, clients have been focused on what they need to do to become compliant with the GDPR as to their E.U. employees and E.U. investors. In addition to updating their vendor contracts, managers have been racing to update their employment documents and subscription agreements to make sure that their latest privacy policies and procedures are known, and that they have the appropriate legal basis to continue to control or process the personal data of their employees and investors.

I have not yet seen clients focus all that much on how the GDPR will affect their abilities to internally research and gather data. It is logical to conclude that the GDPR will impact those abilities because now fund managers need to be much more careful with all types of data they obtain. As a result, with respect to scraping, I think that U.S.-based managers ultimately may be more reluctant to scrape if they are going to come into contact with E.U.-resident personal data.

[See "Best Practices for Private Fund Advisers to Manage the Risks of Big Data and Web Scraping" (Jun. 15, 2017).]

HFLR: If a fund manager takes the appropriate steps in terms of getting the right representations when buying data, will the GDPR force it to change or alter the ways in which it is currently using that data?

Greene: Fund managers will need to alter how they store and hold personal data protected by the GDPR. Sophisticated funds, however, are already careful with personal information. They know how to safely store it and that they need to have internal compliance policies and procedures in place with respect to information security.

As to whether fund managers will need to alter how they use personal data, if they have lawfully obtained the data and are compliant with the GDPR, they should continue to be allowed to make investment decisions on the basis of that data.

HFLR: Whether a fund manager gathers alternative data itself or buys it from a vendor, is the use of anonymized data a way to get around the GDPR requirements?

Greene: Yes, fund managers have always wanted to receive data that has been de-identified and anonymized. The irony is that fund managers have absolutely no interest in PII/personal data or the identification of the individuals to whom that data belongs. For example, they do not care that Jane Doe purchased X dollars of product at Bed Bath & Beyond in the third quarter.

Managers do not want to know who those people are because they know that if they do, then they will have more compliance hoops – in the U.S. and now in the E.U. – to jump through. Thus, when our fund manager clients enter into data-vendor agreements, they include in each agreement a statement to the effect that, "We do not want any personal information. We do not want to know who these people are."

What inevitably happens, however, when you look at, for example, credit card panel data is that there is a stray Social Security number, email address or home address that appears by accident. In that case, there should be a process set forth in the vendor agreement that governs what the vendor will do if an individual's personal information inadvertently makes its way into a data set.

HFLR: How, if at all, will the GDPR's limits and requirements related to automated decision-making impact funds?

Greene: The automated decision needs to involve personal data in order for it to implicate the GDPR's requirements. Therefore, if the adviser takes steps to ensure that it does not come into possession of personal data of E.U. individuals, then the automated decision-making requirements and limits of the GDPR should not apply.

HFLR: Are there other things that fund managers can do to try to ensure that their use of alternative data does not contravene the GDPR?

Greene: What they need to do when buying data is make sure that they obtain robust representations and warranties from data vendors and that they inform vendors that they do not want personal information, including data that can be used to reverse engineer the identity of an E.U. individual. When fund managers are conducting data research on their own (whether on the ground, through a survey or otherwise), they need to ensure that they do not obtain personal information that implicates the GDPR.

The HEDGE FUND LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Vol. 11, No. 24 June 14, 2018

The problem, however, is that because the GDPR defines personal information much more broadly than U.S. law does, fund managers now need to look more closely at offerings from data vendors. They need to examine trials, sample sets of data and dummy sets of data to figure out whether the data does, in fact, provide enough information such that they could reverse engineer the identity of the E.U. persons. If it does, then the GDPR could be implicated.

HFLR: How should fund managers conduct due diligence when selecting data vendors?

Greene: Advisers need to review the samples and dummy sets of data to understand the kinds of data the vendor will provide. They cannot just trust vendors when they say, "We are not going to give you any personal data. We are not going to give you anything that allows you to figure out who Jane Doe is."

A lot of these data companies are very small and not yet up to speed with respect to certain securities and privacy laws. With that said, many are quickly becoming more sophisticated because they see that their counterparty hedge fund manager clients are sophisticated and need to have certain policies and procedures in place from a compliance perspective.

From a vendor due diligence and onboarding perspective, fund managers should add GDPR-related questions to their due diligence questionnaires. Therefore, in addition to asking data vendors questions regarding the purity and provenance of the data they provide; their internal compliance policies and procedures; and their insurance coverage in the event of a data breach, fund managers also need to ask prospective data vendors questions regarding the GDPR.
[For more on managing vendors, see "Fund Managers Must Supervise Third-Party Service Providers or Risk Regulatory Action" (Nov. 16, 2017); "How Fund Managers Can Develop an Effective Third-Party Management Program" (Sep. 21, 2017); and "Study Reveals Weaknesses in Asset Managers' Third-Party and Vendor Risk Management Programs" (Mar. 9, 2017).]

HFLR: If a fund manager has not given any thought to how the GDPR affects its use of alternative data, what should it do immediately?

Greene: Certain E.U. regulators have informally communicated that perhaps they did not necessarily expect absolute compliance on May 25; rather, they want to see an effort to be substantially compliant in the reasonably near future.

Those fund managers that have been focused on their privacy policies, subscription agreements and the personal information of their E.U. employees – and not on what the GDPR means for their use of alternative data – should revisit each agreement they currently have with data vendors. They should reach out to those vendors and confirm that they are not receiving information that implicates the GDPR. Then, they should amend those agreements to add representations to that effect.

To the extent that any vendors are providing data that might put a fund manager within the GDPR's scope, that manager needs to consider whether it wants to stop doing business with that vendor to avoid compliance with the GDPR's requirements.

[See "Best Practices for Due Diligence by Hedge Fund Managers on Research Providers" (Mar. 14, 2013].

---

[1] Personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."