# ALTERNATIVE DATA: WHAT ARE THE REGULATORY RISKS?

From insider trading to GDPR, managers need to navigate a range of issues

BY SAM DALE

Hedge funds are being urged to monitor the compliance risks associated with utilising alternative data as US and EU regulators increasingly focus on this growing area of investment research.

In March, an *HFMWeek* poll revealed more than one-third of readers (37%) are actively harnessing alternative data techniques as part of their investment analysis. In contrast, 40% say they are not utilising any such offerings, while nearly a quarter are starting to experiment.

Alternative data is best defined as non-traditional research that is not price or volume-related but helps predict inputs and outputs better. That could be using technology to measure sentiment on social media, satellite and drone imagery, transactional data for credit cards, mobile phone data and other areas.

Lawyers expect the SEC to take a closer interest in insider trading risks associated with alternative data while the EU's Market Abuse Directive has created a strict environment and the upcoming General Data Protection Regulation (GDPR) will impose new rules on accessing EU citizens' data.

Investors have also begun to take a closer interest in managers' alternative data usage, probing how data is collected and demanding assurances that techniques are compliant and that appropriate due diligence is being conducted on data providers. In a recent survey of hedge fund CCOs by sister title *HFMCompliance*, four in 10 say they have used a third-party alternative data research provider.

"Alternative data providers are currently experiencing a flood of interest in their offerings," says Doug Dannemiller, investment research leader for the Deloitte Center for Financial Services, who recently authored a research paper on the subject. "Just a year ago, these vendors were struggling to gain traction."

Opimas, a consultancy that provides alternative data to managers on a range of subjects, says asset managers are spending 21% more every year on alternative data and that buy-side and sell-side spending could hit $7bn a year by 2020, up from $4bn this year.

## COMPLIANCE RISKS

Experts say much of the legal and compliance landscape surrounding alternative data is undefined as policymakers get to grips with the subject. However, there are some core areas that managers should consider before using alternative data sources and providers. They include insider trading risks, especially with regards to exclusive data sets, alongside breach of contract, privacy, piracy and website terms of use for data scraping and copyright.

"Clients need to be careful the data they are buying is data they are allowed to have," says Peter Greene, partner at Lowenstein Sandler. "That means the original user has given authority [for it] to be used."

Emmett Kilduff, founder of alternative data provider EagleAlpha, says the main questions the firm gets from managers surround the origins of data, privacy policies and the exclusivity of data. He says there are still few legal guidelines around these areas and policies differ from jurisdiction to jurisdiction.

## INSIDER TRADING

Insider trading is the big concern for hedge funds as it can be a criminal offence as well as being a top priority for regulators. "There is a lot of undefined space with alternative data, but venturing into material non-public information (MNPI) is a main concern," says Dannemillller.

The US has a narrow definition of insider trading law where information can be both material and non-public but still might be allowed as long as information has not been misappropriated and no duty has been breached.

Under the EU's market abuse regulation (MAR) that

came into force in July 2016, the use of any price sensitive or material non-public information is banned. Historically the region has taken a tougher stance on this issue. Lawyers say it is harder to buy alternative data in the UK and Europe while some say exclusive data sets are effectively outlawed. In the UK, lawyers say data exclusively sold to one individual or firm is banned. However, if data is made publicly available in some form, even if prohibitively expensive, then it could be allowed.

In the US, if you have what might be considered MNPI related to exclusive or limited data sets then it may be allowed as long as the data was not obtained illegally, but managers are still nervous about usage. The US has also been tough on prosecuting insider trading cases and pursuing regulatory enforcement in recent years. Lawyers say the treatment of alternative data could follow a similar pattern to the regulatory scrutiny of expert networks.

Expert networks provide research to hedge funds often using former employees or close associates of affected firms. The SEC launched a sweeping probe of the networks to investigate if they breached insider trading rules by releasing price sensitive information that was not publicly available. The investigation led hedge funds to rethink how they used them and forced networks to tighten compliance standards.

Greene says: "Alternative data is somewhat comparable to where expert network providers were several years ago. When you meet data providers today, some understand the importance of compliance procedures but not all of them.

"It is very important for legal and compliance to meet with, and certainly talk with, the data provider to ensure the providers understand the issues and their importance. Without that, I would feel very uncomfortable moving forward to contract negotiations and a trial stage."

Hedge fund compliance professionals and lawyers say alternative data is not currently a top priority for the SEC, but that could change.

"We have not seen the SEC take a hard look at it but ultimately regulators are going to want to understand this area and how data is procured," says Greene. "What are you buying? How did you get it? What are you doing with it? Sophisticated managers are not buying anything without looking at it very carefully."

## GDPR

Another major consideration is privacy concerns, particularly in the EU. On 28 May, the GDPR will introduce sweeping new data protection rules for any global firm accessing EU residents' data. The rule requires explicit, continuing consent from all subjects of data, forces firms to provide data breach notifications, monitors the handling of data across borders and requires certain large firms to provide data protection officers. The GDPR has a strict compliance regime that can impose fines of up to 4% of global turnover.

Cyber experts say alternative data providers' anonymised data will generally fall outside the scope of the GDPR but there is uncertainty over how it will apply in certain situations. "Technology is evolving and we are getting better at linking people to data. So it is a very tricky thing to actually decide whether something is personal data or anonymised data," says Sandra Wachter, an Oxford Internet Institute research fellow. "But in general, if you can make sure the data is anonymised the whole GDPR framework wouldn't apply to it at all."

Joe Hancock, cyber-security expert at Mishcon de Reya, says the information that will be defined as personally identifiable is wider than most people realise. "It is very much still an open question," he says. "The regulation says it is name, location data, online identifiers, factors relating to physical, psychological, economic, cultural or social identity so there are really broad applications of this particular act.

"My view is that if you are looking at a person's data having an argument with yourself about whether it is personal or not personal, you are not complying with the spirit of the regulation."

## BEST PRACTICE

Lownestein Sandler's Greene recommends all hedge funds conduct in-depth interviews with data providers they are using to ensure they have a full grip on their compliance procedures.

*HFMCompliance* polling shows that 80% of hedge fund CCOs have been given a veto over all alternative data purchases while 20% will refer the decision depending on the nature of the research. In addition, four in 10 CCOs say they have turned down research over compliance concerns while a further 40% say they have asked for clarifications. Just 20% say they have always been comfortable with the research they have received from providers.

One COO at a sub-$1bn fund in London says the compliance risks are too great to allow his portfolio manager to use such data sources, although this appears to be an extreme viewpoint. As well as an interview, lawyers recommend writing a sophisticated and tight contract in an attempt to ensure there is no MNPI or other compliance concerns.

One general counsel at a $2bn US hedge fund says he always interviews new providers as well as inserting a covenant that no MNPI is associated with the data. "For any new research or data provider, I conduct due diligence on the firm, including speaking to their compliance department if they have one, and insert a covenant in our agreement to say they won't provide us with MNPI or any information in breach of a duty to any third party," he says.

"For an alternative data provider, I would also review any data being sent to our analysts before the analysts receive the data."

Igor Gonta, CEO of alt data provider MarketProphit says there is a difference between large and small funds in how seriously they take compliance checks. "Larger funds are definitely very serious about their compliance," he says. "They will have in-depth discussions to understand how it is being collected, where it is coming from and ensuring it is anonymised."

Gonta adds agreements are not standardised because it is a new area and the data is very different from source to source, for instance drone imagery to social media tracking.

Deloitte also suggests hedge funds should consider modifying investor disclosures about investment policy and processes when using alternative data.

In addition, vendors are starting to offer compliance software and procedure recommendations to support investment managers in determining that their alternative data use is regulatory-ready, although managers warn such tools can vary in quality and do not outsource regulatory responsibilities when looking to harness such data. Regulations are not evolving as quickly as the technology but this could change very soon. ■