EU DATA PRIVACY ALERT – October 2011

WHAT YOU NEED TO KNOW ABOUT QUICKLY EVOLVING EU DATA PRIVACY LAWS AND ENFORCEMENT

The EU has been at the forefront of global data privacy since 1995. The EU Data Protection Directive 95/46/EC (the Directive) and national legislation implemented in EU Member States, like the UK Data Protection Act 1998 (DPA), provide broad definitions of "Personal Data" and who is deemed to be a "Data Controller," ensuring that virtually all background due diligence companies and their clients, such as banks, pension funds, hedge funds and consultants, are caught in the net of the EU data privacy laws. As will be explained, what is covered under the DPA is far broader than what investigative firms likely thought; rather than relating solely to identifying information that if mishandled could lead to identity theft, the gathering of background information itself (under the scenarios laid out below) is subject to these laws.

For years, sporadic enforcement and ineffective penalties for non-compliance resulted in disinterest in going through the steps required to be in legal compliance. This lackadaisical enforcement environment has changed dramatically in the aftermath of the global banking crisis, massive hedge fund frauds and the Great Recession.

European nations have increased fines for non-compliance by up to 100 fold: In the UK, for example, fines for violating the DPA increased from a maximum £5,000 to up to £500,000. Although the maximum fine has yet to be imposed in the UK, there have been a number of fines around the £100,000 level along with recent comment by the UK data protection authority (ICO) on the need to introduce prison sentences for severe breaches. Violation of the French equivalent data protection legislation includes criminal sanctions of up to 5 years imprisonment and fines of up to €1,500,000, as well as administrative sanctions by the French data protection authority, the CNIL (up to €150,000 for a first time offender). Substantial fines and penalties are in place throughout Europe, but with noticeable differences in the approach of data protection authorities. A recent case in Spain resulted in a fine of €300,000 for loss of data by one data controller, whereas in Greece, a fine of €8,000 was imposed for a similar breach.

Although the stated intent of the Directive is protection of information, some commentators have suggested that such enforcement measures and fines serve as a source of new revenues for cash-strapped European governments. Moreover, enforcement agencies throughout Europe are eager to prove to the public they are on the ball, and as a result enforcement actions have skyrocketed. Whatever the reason, if you are a hedge fund due diligence company or you are ordering reports from such companies, it is just a matter of time before you will have governmental regulators reviewing your procedures, with potentially devastating fines and penalties for material non-compliance.

Here is a quick overview of what you need to know.

1. The EU Directive, as it is implemented by each EU Member State, defines "Personal Data" broadly. If you are collecting data on an individual (known under the legislation

as a "Data Subject"), then it is likely that such information will be deemed to be Personal Data. Publically available personal data is still Personal Data, even if it can be found on a Data Subject's website or social media sites. The Directive and national legislation will still apply. There are additional steps to take if the data is "Sensitive Personal Data", as defined by the Directive and Data Controllers should be aware of these, if processing data relating to Data Subjects' health, sex life, trade union membership, religion, criminal record and ethnic origin.

2. If you are collecting Personal Data and have any degree of control over that data, such as putting it into a background report or deciding what to do with such information (something all funds of funds and most consultants certainly do), then likely you will be deemed to be a "Data Controller." Therefore, hedge fund due diligence companies **AND** their clients, are often found to be Data Controllers. If you are merely collecting the personal data for a third-party, and don't in any way control the data, you still have obligations under the DPA as a "Data Processor."

3. Prior to collection and/or dissemination of Personal Data, the "Data Controller" must:

a. Fully disclose in writing to its Data Subjects the categories of information it will collect;

b. Fully disclose how the information will be utilized and transmitted; and

c. Obtain the Data Subject's express written consent to such collection and usage of the data.

<u>I get it, but getting releases still seems like a giant pain …</u>

Because a potential investment into a Data Subject's hedge fund may be contingent upon a third-party background report, the Data Subject often actually wants the potential investor to get the report. However, requiring the hedge fund Data Subject to review and sign a legal disclosure and consent form, as a condition to getting a report processed can seem burdensome. As discussed above, the lack of enforcement over the years and the fact that many background companies are out of compliance gives the Data Subject and its potential investors the impression that the request is an unnecessary imposition.

The potential investor may tell the due diligence company that "no one else requires this so if you make us sign then we'll take our background business elsewhere." But the minor inconvenience of requiring the Data Subject to sign the consent must be measured against the current regulatory environment and extreme legal implications that can arise from non-compliance. Both the risk and cost of audit/enforcement action is higher than ever. It's a "bet the company" risk. Is the consent requirement not a small price well worth paying to cut your risk? The purpose of a due diligence report is mitigating risks. It seems incredulous that you or your client would be willing to subject itself to such risks.

But how will I answer subject questions?

As for the Data Subject, most release questions are readily resolved once the Data Subject understands that the law exists for THEIR protection, that non-compliance puts its potential client at severe legal risk, and that a consent should take no more than a few minutes to read, sign and fax or email back. If despite this explanation you have a Data Subject who continues to object, perhaps there are other reasons for such resistance. Maybe the Data Subject does not want a report ordered because of a negative history.

Laws are fluid

Please note that the law is changing constantly and the Directive is implemented uniquely in each European country. Certain countries require advance registration. If data is to be transferred to countries outside of the European Economic Area, there are strict requirements. Data Controllers have certain obligations as it relates to data security. Although this article has focused on the EU Directive, many countries throughout the world have some form of Data Privacy laws. If you are collecting data anywhere in the world, qualified legal counsel should conduct a thorough case-by-case analysis. Do not rely on this article for legal advice.

Arnie Herz is a U.S. based business lawyer with over 20 years of experience. He has a strong international practice focused on business issues, intellectual property and data privacy. Mr. Herz is also a business mediator and is a member of the Mediation Panel of Federal and State Courts in New York City. He can be reached at arnie@arnieherz.com.