Managing Privacy Risks in E-Discovery Data Collection and Processing: Understanding data privacy regulations for personally identifiable information

Properly managing the personally identifiable information (PII) of employees and customers has become a primary concern for corporate counsel and risk managers. It's no wonder given the massive fines regulators are dishing out. In 2012, the Federal Trade Commission fined Google $22.5 million for misrepresenting the information it collects on its users. More recently, the Federal Communications Commission slapped a $25 million fine on AT&T stemming from the company's lax internal data security practices that allowed the Social Security numbers of more than 200,000 customers to be accessed and sold to criminal organizations.

As a result, most companies have tightened the controls in the daily operation for privacy compliance. One area that is still often neglected, however, is electronic discovery, when the legal team, often with third party assistance, collects and transfers large amounts of PII for production in legal matters.

Whether for litigation or an investigation, PII is often collected and processed by numerous parties, making it subject to multiple privacy regulations both domestically and internationally. For example, the U.S. provides privacy protections to U.S. citizens, U.S. persons, and to some degree non-U.S. citizens through numerous—and some would argue disjointed —frameworks at both the state and national level.

Conversely, the EU consolidates its privacy laws and applies them across member states. Counsel and risk managers may not always be aware of the numerous regulations governing the data they are collecting for litigation holds or investigations. As a general practice, they should have in place safe guards and procedures that recognize the types of data being collected and transferred externally to a data processing group.

PII

Underlying all data privacy regulations, both in the U.S. and abroad, is protecting PII. PII includes any individual pieces of information that may be used to identify a single person; most generally this can be a person's name along with one additional piece of information such as a driver's license number or credit card number. Within the U.S., the definition of PII varies across the numerous controlling regulations, with some definitions differing based on the underlying regulations subject matter or location. For example, within the financial industry, the Gramm Leach Bliley Act's (GLBA) three separate rules govern the use, protection, and dissemination of non-public personal information. At the state level, many states go beyond the most basic definition of PII and call for protection of additional combinations of information including unique biometric data (Connecticut), passwords unconnected to a name (Georgia), and taxpayer identification numbers (Maryland). Additionally, some states such as Massachusetts have passed regulations requiring encryption and specific technical standards for any entity that collects and stores information about a resident of Massachusetts. For litigants in states with local rules (or with matters touching these states), compliance must continue during discovery.

For many organizations that do business internationally, their understanding of privacy compliance has to extend beyond U.S. borders.

Collecting EU personal data

U.S. legal matters often call for the discovery of data regarding EU citizens. When posed with this issue, counsel has three limited means to transfer personal data from the EU to the U.S.: the EU-U.S. Privacy Shield, Binding Corporate Rules, and Standard Contractual Clauses. Each has its own limitations and varying degrees of difficultly and expense, but it is critical to know how to deal with transferring this information long before you face a discovery deadline.

The Privacy Shield provides one mechanism for registered companies to legitimately transfer data to the U.S. from the EU. It is available to any organization whose activities are regulated under the Federal Trade Commission or the Department of Transportation, which excludes banks, for example. To comply with the Privacy Shield, organizations must undertake an internal self-assessment and then certify online with the Department of Commerce (DOC). The DOC will review the documentation provided by the organization and potentially request additional documentation. Organizations are also required to renew their certification with the DOC annually. Once registered, companies can then legally transfer any of the data types described in their registration, so long as they live up to their promises and obligations to protect it.

However, the future of Privacy Shield remains precarious at best, and it may not be the most reliable choice for counsel. Some proponents of the Privacy Shield believe it will be able to withstand any future challenges like those that disqualified its predecessor, Safe Harbor. Others have challenged that the new Privacy Shield is too vague and lacks the robustness necessary to withstand future challenges in court.

Binding Corporate Rules (BCR) were created by the Article 29 Working Party, an independent advisory body on data privacy issues within the EU, as a means for multi-national companies to transfer personal data within their organizations and between certain sub-entities. BCRs are developed within an organization based on EU privacy standards. Then they are approved by a lead data protection authority after review and comments from each jurisdiction's data protection authority. At present, around 90 global companies have received approval to implement their own versions of BCRs. These rules will apply across the organization regardless of location, and will require ongoing cooperation with EU data protection authorities, which some have argued is burdensome. The organization will also be subject to external audits to ensure continued compliance.

Despite these onerous-sounding requirements, once in place, BCRs ensure there is a clearly defined process for data transfers within a corporation without having to reinvent the wheel with each necessary data transfer. However, BCRs are not for every company, as the approval process can be lengthy and expensive. Additionally, depending on the countries involved, there can be additional compliance hurdles with each data transfer. Most importantly, BCRs are typically silent on and not intended to control onward transfers to third parties outside the original company. For this reason, while they may facilitate transfers of data across boarders within the company, they are typically unsuitable for transfers for discovery purposes where the data will be disclosed to additional parties and the courts themselves.

The best option for counsel is the Standard Contractual Clauses (SCC). SCCs offer the ability to comply with EU data privacy laws on a contract-by-contract basis using known contract language, which is pre-approved for use in data transfers outside of the EU. These are often the preferred method for service providers, as the parties involved are already negotiating a service contract. The SCCs are listed on the European Commission's website, and can be directly copied into contracts to ensure compliance with EU data privacy laws. Additionally, in the event that the Privacy Shield is invalidated in the future, the contractual obligations between the parties in SCCs will still stand. SCCs can be modified for a particular organization's needs, but may require additional approval from the relevant DPAs prior to being enforceable if modified.

There's one thing to note: SCCs are being challenged in Ireland as providing inadequate protection, which may ultimately invalidate their use as a means of data transfer outside of the EU, but this is ultimately unlikely. If anything the templates may simply be updated at some point for use in future agreements.

Compliance and Risk Management Tools

There is no single best method to limit privacy risk exposure. The numerous laws surrounding data privacy make it critical for counsel to know what data is being collected, what information is contained in the stored data, and where it is geographically located.

One approach we recommend involves building a privacy data map. A privacy data map will identify the scope of data sources and repositories, and includes the locations and types of data being stored by the company across all offices and external locations, including offline data archives and third-party data service providers. A map can prove a valuable resource when you are crafting new discovery plans and deciding what data needs to be collected and transferred.

Counsel should also inquire into the existing contractual agreements with all third-party service providers to ensure compliance with current data privacy standards and regulations. Most e-discovery providers will have standard data handling processes and procedures. These can include encryption requirements on sensitive information, security standards for specific data regulations such as data subject to the International Traffic in Arms Regulations, as well as custom solutions to redact or mask certain types of data, like Social Security numbers.

Maintaining documentation surrounding data privacy and ensuring downstream compliance will place counsel in a better position when they are implementing litigation holds or responding to investigation requests. However, recent court challenges and the subsequent uncertainty with EU laws regulating personal data transfers have posed particularly challenging hurdles.

Logistics in Collection and Processing

Once litigation is reasonably anticipated, counsel should consider logistics in advance of data collection and processing. For example, you might engage an e-discovery provider who can process data at a local site in the EU in an effort to minimize the amount of data needing transfer. This will keep things moving forward while you work to put in place contracts or alternative arrangements with non-EU service providers.

You might also consider working with local experts on managing the preservation and collection process. Local data authorities may have more or less demanding requirements based on their interpretations of the EU data privacy regulations, which might otherwise be unclear to outsiders.

Regardless of geographic scope, during the meet and confer, counsel should consider negotiating limitations or culling criteria that can further limit the amount of data being collected or processed. Once data has been identified as potentially relevant, you should work with an e-discovery provider who can implement various technologies to assist with privacy compliance. For example, structured or fielded data such as home phone numbers and Social Security numbers can be auto-redacted or masked in bulk. Additionally, certain types of records, such as those produced from human resources or health-providers, can be segregated for review by a limited number of people and with special access controls. For data with unknown content, counsel can start the identification process by reviewing the pertinent regulations' definitions of PII, and then work to identify the formats typically used by the company to record information such as phone numbers, birthdays, or credit card numbers. In some instances, data analytics can also identify content-driven personal information, such as doctor's notes.

Data mining techniques and PII identification software are steadily improving, but data privacy is a rapidly changing constellation of rules and regulations that don't always mesh with the demands of litigation or investigations. It is counsel's responsibility to understand the varied umbrellas of compliance both for the data it creates in the process of doing business, as well as the data it collects and processes for litigation or any other business activity. Careful planning and preparation can go a long way before you face data privacy issues in the regular course of business and litigation.

AlixPartners LLP
Patron

Candice Lang

Topics

Featured Topics:
Personally Indentifiable Information (PII)
Other Topics:
EU Data Privacy
Web Topics:
AlixPartners