Data privacy basics – what type of information is regulated?

By Carol Umhoefer and Jennifer Kashatus

Virtually every company maintains some personal information – your company might hold personal information about employees, customers, or both. Whatever personal information your company possesses, your company should take measures – and, in fact, may be required by law to take measures – to protect that information. To appropriately handle personal information and to protect one of your most valuable assets – information – take stock of the information that your company maintains as the starting point to getting your privacy house in order.

What is PII and personal data?

In the US you've heard of "PII" – Personally Identifiable Information, information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Outside the US, the same concept is usually denoted by the term "personal data" – data relating to an identified or identifiable natural person.

Clearly, knowing whether you are collecting and processing PII or personal data is the first step in understanding whether and how you are bound by data protection requirements. But there are times when it is not clear whether data rises to the level of personal data and must be regulated as such. In practice, knowing when a natural person is identifiable may not be as simple as it seems.

Is an IP address subject to privacy regulations?

An IP address identifies a device, and whether static or dynamic, an IP address will change over time. In the EU, regulators have pretty consistently considered that an IP address (even a dynamic address) identifies a person. Some regulators have advised hashing a fixed number of digits in each IP address in order that it not identify a person. Courts, on the other hand, have in some cases refused to order criminal penalties for activities associated with an IP address – although the device may have been implicated in criminal activities, the owner of the device is not proved guilty on the mere basis of use of his IP address.

Is geolocation data subject to privacy regulations?

At some point, geolocation can be sufficiently precise, or abundant, to identify a person. Or the geolocation data may not be precise but when it is associated with other data it may serve to identify an individual. The same reasoning can be applied to nearly any potential identifier; in a dense urban neighborhood a zip code will correspond to tens of thousands of persons and need to be correlated to a host of other data in order to identify a person, whereas in remote areas a zip code alone may designate a single individual.

Can data be made generic so that it is not subject to privacy regulations?

Anonymization of personal data is often seen as the holy grail of "compliance," since anonymous data is not subject to data protection laws. Yet achieving true, irrevocable anonymity is often difficult, and regulators may pay close attention to claims that data is anonymous. There's an abundance of literature on what anonymous data is, and what it isn't. Generally speaking, pseudonymized data (*eg*, substituting a code for a name), or data where direct identifiers have been removed, will *not* be considered anonymous. Faced with a skeptical regulator, the prudent approach will usually consist of treating pseudonymized and de-identified data as personal data and affording it all the protections required by law.

What steps should a company take to comply with applicable privacy laws?

To put your company in the best position to comply with privacy regulations, and, perhaps more importantly, to ensure that your company is able to appropriately protect the data in its possession, your company should take stock of the data in its possession. Take the time to understand, as a starting point:

- What types of personal information does your company maintain about employees and or customers?
- Where does your company store that information and which employees or classes of employees have access to that information? and
- Under what circumstances does your company share that information with third parties?

Take the time to understand what your company already has done to address privacy and data protection. For example:

- Does your company have internal policies and procedures to protect personal information?
- Does your company have an incident response plan in the event of a data breach?
- Does your company require third party service providers to safeguard your information?
- Does your company have a privacy policy?
- Is each of the above items up-to-date?

Once you have identified what you might already have in place, next consider whether your company is in the best position to protect its data. For example, consider whether all of the employees that have access to personal information really need that personal information to perform their jobs. Similarly evaluate whether your third party service provider needs all of the information that you are providing to it – and at the same time, evaluate whether your third party service provider has appropriate security in place to protect your information, a valued asset. Then check to see whether your privacy policies and procedures are accurate and up-to-date, and, even if not, whether there are ways in which you can modify your procedures and policies so as to protect the information that is in your company's possession.
