CEP Magazine - May 2020
Is it wise to keep personal data for longer than necessary?

By Robert Bond

Robert Bond (robert.bond@bristows.com) is Partner & Notary Public at Bristows LLP in London, UK.

As data protection laws continue to evolve around the world, one of the core data protection principles—storage limitation—remains a priority. It requires organizations to retain personal data for only as long as it is necessary for the purposes for which they are required. The challenge is that the necessary amount of time has not been defined.

The European Union General Data Protection Regulation provides specific requirements for the storage limitation principle, saying that personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."[1]

If data are truly the "oil of the internet," then they have value. That's why businesses often keep data for as long as possible, saying that they never know when the data might be useful. However, keeping personal data longer than is necessary turns that information into toxic data. If leaked, they can have disastrous consequences not only for the individuals whose data are uncontrolled but also for the business that loses control of the same data.

Establishing a robust data retention policy requires businesses to fully understand the "who, what, where, when, why, and how" of the personal information that they collect, use, and retain. Good data governance enables a business to demonstrate the provenance of that information. It also demonstrates the key principle of accountability under many data protection laws.

Depending on the nature of your business, the legal and regulatory demands relating to the retention of personal data will vary. In addition to sectorial requirements, there are jurisdictional variations that make the issue of data retention even more complex, especially for multinational businesses.

In an increasingly litigious world, any data retention policy needs to respect and understand the requirement for "litigation hold." It requires data to be "quarantined" during the course of a litigation or an investigation. Therefore, any data retention policy must interface with data destruction procedures.

Developing a comprehensive data retention policy is a significant exercise for many businesses. It often gets put on hold as seemingly too difficult, and it is only when things go wrong that the compliance professionals, as well as the business itself, wish that they had established it sooner!

1 Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119., Article 5 (1)(e). https://bit.ly/2xcYeX3