The impact of the GDPR on the retention of personal data

Finding the right balance between business needs and privacy rights is an even more important compliance issue because the General Data Protection Regulation ('GDPR') directly and indirectly requires businesses to limit the collection and storage of personal data. In this article, William Long and Vishnu Shankar of Sidley Austin LLP discuss the likely impact of the GDPR on retention and storage of EU-originating personal data.

The new 'storage limitation' rules in the GDPR may make it more challenging for businesses to carry out processing activities that are dependent on either long term or large data storage[1]. In addition, businesses will have to weigh the benefits of storage against the possible liabilities arising from failing to comply with other GDPR obligations arising from such storage, such as the risk of security breaches and enforcement action. The GDPR more closely intertwines the issues of data retention and cyber security.

Storage limitation principle

The current EU Data Protection Directive 95/EC/46 (the 'Directive') requires businesses to minimise the retention of personal data such that data must be kept in a form that permits identification for no longer than necessary for the purposes for which the data are collected or processed[2]. The GDPR, which will replace the Directive and all national implementing legislation in May 2018, expands on this principle by providing that in order to comply with the 'storage limitation' and 'data minimisation' principle, data controllers must ensure that 'the period for which the personal data are stored is limited to a strict minimum[3].' (There are narrow exceptions for certain archiving activities for scientific or historical research or for statistical purposes.) Effectively, in order to comply with the 'storage limitation' principle businesses must affirmatively delete or return personal data - or retain data such that it is not 'personal' - if retaining such data is not essential for the purposes for which the data was collected[4].

EU data protection authorities are able to impose more burdensome sanctions under the GDPR. Failure to comply with the 'storage limitation' principle or violating the rights of individuals (a data security breach as a result of storing data, for example) may result in fines as high as 4% of annual worldwide turnover or €20m - whichever is the greater. Therefore, consideration as to the appropriate approach to data storage is a key compliance issue.

Storage limitation in practice

The 'storage limitation' principle in the GDPR may require businesses that act as data controllers to:

- Provide information to individuals on applicable retention periods or the criteria to determine such periods, for example, in privacy notices prior to collection[5]. In practice, it may be easier to identify the criteria than specify the retention period. In addition, once specific storage periods have been notified, there may be less flexibility to modify such periods;
- Determine the storage period based on the purposes for which the business is holding the information. This requires consideration of the 'data minimisation' principle, which is connected to storage limitation, and requires that:
  - the storage period be a 'strict minimum[6],' and tied to the accomplishment of the stated purposes[7]. This means that data cannot be retained because a new purpose might be found in future;
  - the retention and processing of personal data may, in general, be justified only 'if the purpose of the processing could not reasonably be fulfilled by other means[8].' This is a reflection of the 'privacy by design and by default' principle. It requires privacy considerations and privacy enhancing measures to be incorporated during the planning and execution of data processing activities. A security breach that involves pseudo-anonymised data for instance improves the likelihood that a security breach will not have to be notified to regulators or individuals; and
  - time-limits for erasure and periodic review be established to ensure that data is not being stored where unnecessary[9]. Even if storage periods have been established, businesses are advised to review whether it is still necessary to retain such data before the expiry of the storage period. This may arise when the purpose of the processing is accomplished sooner than expected.
- Securely delete data in accordance with written retention periods and information security and retention policies. Storage is not recommended, unless one of the narrow exceptions apply. Non-compliance with such policies may result in regulatory action;
- Where possible keep detailed records of retention periods if acting as a data controller[10]. The GDPR places emphasis on record-keeping, and controllers may need to demonstrate through records that due consideration was given to determining storage periods, data security and data deletion; and
- Data processing contracts with data processors must contain terms requiring the processor to delete or return all personal data to the data controller at the end of provision of the services relating to the

processing[11] or on request.

Other GDPR obligations

The issue of data storage is not solely associated with the 'storage limitation' principle. In fact, even if a business is able to store personal data without breaching the 'storage limitation' principle, in a strict sense, there may be other reasons for the business not storing data, at least, on a more long term basis, given that if a business stores personal data it potentially becomes subject to certain other obligations in the GDPR, such as:

- Data security: This is a key consideration in relation to data storage because of the risks of security breaches. In particular, the GDPR contains enhanced data security obligations relative to the Directive. In addition to the general data security standards, businesses may, in some circumstances, have to adopt specific security measures to protect data that is stored such as encryption and business continuity/disaster recovery and IT testing mechanisms[12]. Further, unlike the Directive which did not require notification to regulators or individuals in the event of a breach, under the GDPR, notifications may be required, depending on the level of risk[13].
- 'Subject access right' and 'data portability': As in the Directive, under the GDPR, individuals are able to request from data controllers access to data that the controller has stored. However, the GDPR has enhanced this 'subject access right[14]' most notably through introducing 'data portability[15].' Individuals are now able to exercise their 'subject access right' by obtaining copies of their personal data in a machine-readable format and can require that their data be transferred to an alternate data controller. In practice, this 'subject access right' coupled with 'data portability' may be difficult and expensive to implement for a data controller that stores large amounts of data on a long term basis.
- Right 'to be forgotten' and right to object to processing: Each of these related rights allow an individual, under specified circumstances, to require a data controller to erase personal data, restrict the processing or stop the processing of personal data[16]. Like with the 'subject access right,' these rights may be difficult in practice and expensive and will need to be considered by businesses when implementing the GDPR.
- Restrictions on profiling and automated decision-making: Like the Directive, the GDPR imposes restrictions on automated data processing activities that result in legal or adverse effects on individuals[17], particularly where sensitive personal data or children are involved. The GDPR's restrictions on certain Big Data analytics, may dis-incentivise data storage because, in many instances, the purpose of long term/large data storage is to enable analytics.

By enhancing data controllers' obligations around data security and the rights of individuals together with greater potential enforcement, such restrictions will dis-incentivise long term storage of personal data

Conclusions

The GDPR imposes substantial obligations on data controllers who wish to store personal data. The obligations impose not only substantive obligations (such as strict storage periods), but also procedural obligations (such as requiring 'privacy by design and default' accountability measures). Businesses will need effective compliance mechanisms to adapt to these new retention requirements. In addition, by enhancing data controllers' obligations around data security and the rights of individuals together with greater potential enforcement, such restrictions will dis-incentivise long term storage of personal data. In particular, the increasing risks of data breaches coupled with the higher likelihood of enforcement action and litigation may nudge businesses to more proactively securely erase personal data.

William Long Partner
Vishnu Shankar Associate
Sidley Austin LLP, London
wlong@sidley.com

1. Further, on an EU Member State-level, Member State attempts to require providers of electronic communications services to store certain personal data for access by public authorities have culminated in two cases (Tele2 Sverige AB (C-203/15) and Watson (C-698/15)) before the CJEU. Decisions in these cases are expected to determine whether, and if so, under what circumstances and subject to what safeguards, Member States can require the storage of, and access to, such data by public authorities.
2. Art. 6(1)(e), Directive.
3. Recital 39, GDPR.
4. Art. 5(1)(e) GDPR.
5. Art. 13(2)(a), GDPR.
6. Recital 39, GDPR.
7. Exceptions apply to archival, scientific, historical and statistical activities.
8. Recital 39, GDPR.
9. Recital 39, GDPR.
10. Art. 30(1)(f), GDPR.
11. Art. 28(3)(g), GDPR.
12. Art. 32, GDPR.
13. Arts. 33-34, GDPR.
14. Arts. 33-34, GDPR.
15. Art. 20, GDPR.
16. Arts. 17, 18 and 21, GDPR.
17. Art. 22, GDPR.