

Exploring recent anonymisation guidance

05/08/2016

Commercial analysis: The UK Anonymisation Network's recent publication of the Anonymisation Decision-Making Framework provides guidance and practical advice to businesses on how the practice can be used to meet their operational needs. William Long, partner, and Francesca Blythe, associate, at Sidley Austin LLP, discuss the suggestions.

Is there a legal obligation to anonymise data under the Data Protection Act 1998 (DPA 1998), the General Data Protection Regulation (GDPR) or other legislation?

There is no legal obligation to anonymise data under [DPA 1998](#), the GDPR ([Regulation \(EU\) 2016/679](#)) or any other relevant legislation in the UK. However, it should be noted that to the extent data are anonymised then this data will not be subject to the provisions of [DPA 1998](#) and/or the GDPR.

In addition, under the GDPR, pseudonymised data will be considered a form of personal data and therefore be subject to the provisions of the GDPR. This is because pseudonymised data can be attributed to a natural person by the use of additional information allowing for re-identification of the individual. The processing of pseudonymous data is actively encouraged under the GDPR and pseudonymisation is identified as a means of implementing appropriate safeguards to protect personal data. For example, GDPR, art 6(4) states that the pseudonymisation of data will be a factor controllers should consider when determining compatibility of purpose for further processing and GDPR, art 25(1) includes pseudonymisation as an example of a measure which may satisfy requirements to implement data privacy by design.

What is the nature of the guidance?

The guidance is aimed at individuals in organisations who need a practical guide to anonymisation. It is intended to give practical advice to businesses on how anonymisation can be used to meet their operational needs. However, the guidance document does not impose any legal obligations, although as per existing guidelines on anonymisation from the UK's Information Commissioner's Office (ICO), it is intended to encourage good practice.

Is the guidance GDPR-compliant?

According to the UK's new information commissioner, Elizabeth Denham, the approach taken in the guidance is fully consistent with the provisions under the GDPR.

How does it tie in with guidance produced by the ICO?

This guidance is not intended to replace the ICO guidance but is to be used as a tool alongside it.

What types of anonymisation are typically used?

The following types of anonymisation techniques are typically used by organisations:

- formal anonymisation—this is where direct identifiers are removed from a data set or masked in some way so that the person cannot be identified
- guaranteed anonymisation—this technique ensures that there is no risk of an individual being identified within a dataset (this is useful as it mitigates the risk of re-identification, but in order to achieve guaranteed anonymisation, the data is often rendered useless)
- statistical anonymisation—this technique does not aim to reduce the chance of re-identification to zero but looks to control or limit the chance of disclosure (this technique brings anonymisation in line with business risk management)
- functional anonymisation—this is the favoured approach in the guidance, as it incorporates characteristics of statistical anonymisation into a format that is more tailored to the organisation

In reality, the guidance makes it clear that there is no one technique to anonymise data. How data is anonymised will depend on the data and the overall context. There is no one technique that works for every organisation.

What guidance is given for organisations that are looking to anonymise personal data?

The guidance is split into two main chapters. The first gives an overview about:

- what anonymisation is
- looking at the law
- the types of anonymisation
- controlling disclosure
- anonymisation solutions, and
- the importance of ethics in anonymisation

The other main chapter looks at the anonymisation decision-making framework focusing on data situation audits, disclosure risk assessment and control and impact management. The appendices to the guidance set out example scenarios and methods for anonymising data. The guidance helps organisations to strike a balance between access to information and the need for privacy through the use of anonymisation techniques.

William Long is a partner at Sidley Austin LLP, where he advises international clients on a wide variety of data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the European advisory board of the International Association of Privacy Professionals and has experience with EU and international data protection and e-commerce projects working for clients in financial services and life sciences, as well as other sectors.

Francesca Blythe is an associate at Sidley Austin LLP, where she advises international clients on a wide range of data protection and privacy issues and the implementation of data protection compliance projects. Her main areas of practice are data protection, privacy, e-commerce and information technology.

Interviewed by Jane Crinnion.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor



CLICK HERE FOR
A FREE TRIAL OF
LEXIS®PSL

About LexisNexis | Terms & Conditions | Privacy & Cookies Policy
Copyright © 2015 LexisNexis. All rights reserved.