The UK Data Protection Authority issues a Code of practice on anonymization

In November 2012, the UK Information Commissioner’s Office (ICO) published a Code of Practice on managing data protection risks related to anonymization. This Code provides a framework for organisations considering using anonymization and explains what it expects from organisations using such processors.

One of the benefits of anonymization is that the onerous data protection obligations under EU data protection laws, including the UK’s Data Protection Act 1998, will not apply to data rendered anonymous such that individuals are no longer identifiable.

As the Code notes, anonymization can allow organisations to make information derived from personal data available in a form that is rich and usable whilst protecting individuals.

The main good practices and recommendations provided in the Code are summarised below:

- **Personal data, anonymization and identification**: the Code highlights that the concept of “identify” and therefore “anonymized” is not straightforward because individuals can be identified in numerous ways and re-identification by a third party can also take place. It is therefore crucial for businesses to assess the risk of identification when they decide to disclose anonymized data.

- **Ensuring effectiveness of anonymization**: the ICO recommends the use of the “motivated intruder” test to assess the risk of re-identification. This test involves determining whether a “motivated intruder”, who is a person who starts without any prior knowledge but wishes to identify the individual from whose personal data the anonymized data has been derived, would be successful. It can be done by (i) carrying out a web search to verify if date of birth and postcode can lead to the identification of a specific individual; or (ii) using social networks to establish if anonymized data can lead to an individual’s profile.

- **Consent**: importantly, the Code provides that consent is generally not needed to legitimize an anonymization process as it could be logistically onerous or even be impossible to obtain such consent.

- **Governance**: organisations using anonymization should have in place an effective and comprehensive governance structure that should include (i) a Senior Information Risk Owner (SIRO) with the technical and legal understanding to manage the process, (ii) staff trained to have a clear understanding of anonymization techniques, the risks involved and the means to mitigate them, (iii) procedures for identifying cases where anonymization may be problematic or difficult to achieve in practice, (iv) knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymization, (v) a joint approach with other organisations in their sector or those doing similar work, (vi) use of a privacy impact assessment, (vii) clear information on the organization’s approach on anonymization including how personal data is anonymized and the purpose of the anonymization, the techniques used and whether or not the individual has a choice over the anonymization of its
personal data, (viii) review of the consequences of the anonymization programme, and (ix) a disaster recovery procedure should re-identification take place and the individual privacy is compromised.

- **Trusted Third Party:** a Trusted Third Party is an organisation which can be used to convert personal data into anonymized data. The Code highlights the value of using a Trusted Third Party arrangement especially where a number of organisations each want to anonymize personal data they hold for use as part of a collaborative project. Use of Trusted Third Party arrangements can facilitate large scale research using data collected by a number of organisations without the organisations involved ever having to access each others’ personal data. It also allows researchers to use anonymized data when the use of personal data is not necessary or appropriate, and can be used to link datasets from separate organisations to create anonymized records for researchers.

The Code also clarifies when the research exemption under the UK Data Protection Act can be relied upon to process personal data for research purposes and concludes with explanations of key anonymization techniques and various case studies such as one on the use of anonymization in clinical studies.

The Code which also sets out other good practices and recommendations is welcome having been published at a time when anonymization techniques and the status of anonymized data are key issues for many industries including digital media, financial services and life sciences. Anonymization and the ability to use data will also remain key issues with the current discussions on the proposed EU Data Protection Regulation and clarity on these issues at an EU level would also be welcome.

For further details on anonymization of personal data please contact William Long (wlong@sidley.com) or John Casanova (jcasanova@sidley.com).

**The Privacy, Data Security & Information Law Practice of Sidley Austin LLP**

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property, and criminal issues. Sidley provides services in the following areas:

- Privacy and Consumer Protection Litigation, Enforcement and Regulatory Compliance
- Data Breach, Incident Response, and Cybersecurity Advice
- Global Data Protection, International Data Transfer Solutions and Cross-Border Issues
- Corporate Data Protection, Compliance Programs and Information Governance Assessments
- FTC and State Attorney General Investigations of Unfair or Deceptive Acts and Practices
- Social Media, Cloud Computing, Online Advertising, E-Commerce and Internet Issues
- EU, China and Japan Data Protection and Compliance Counseling
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Communications Law and Data Protection
- Workplace Privacy and Employee Monitoring
- Website Policies Online Trademarks and Domain Name Protection
- Records Retention, Electronic Discovery, Government Access and National Security

To receive future copies of this and other Sidley updates via email, please sign up at [www.sidley.com/subscribe](http://www.sidley.com/subscribe)