What does the revision of the OECD Privacy Guidelines mean for businesses?

The Organization for Economic Cooperation and Development (“OECD”) has long recognized the importance of privacy as a condition for the free flow of personal data across borders. Monika Kuschewsky examines what impact the revision of the OECD’s Privacy Guidelines will have on businesses.

Monika Kuschewsky

Monika Kuschewsky, a German qualified lawyer and certified privacy professional, is Special Counsel in Covington & Burling LLP’s global Privacy & Security practice. Monika, who is based in Brussels, has broad experience in a wide range of data protection matters which are relevant to global companies, with a particular focus on international data transfers, outsourcing, HR and direct marketing. She also advises on the data protection implications of the use of new technologies and practices, such as Big Data, BYOD (Bring Your Own Device), cloud computing, geolocation services, cookies and social networks.

MLex’s online market intelligence services have become indispensable primary resources for anyone requiring reliable, comprehensive, real-time intelligence, commentary and analysis about the impact of regulation on businesses around the world.

MLex customer services +44 (203) 402 7000
customerservices@mlex.com – www.mlex.com
The Organization for Economic Cooperation and Development (“OECD”) has long recognized the importance of privacy as a condition for the free flow of personal data across borders. Monika Kuschewsky examines what impact the revision of the OECD’s Privacy Guidelines will have on businesses.

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the “Guidelines”), published by the OECD in 1980, were one of the earliest initiatives in the area of data protection. The Guidelines were adopted to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders.

Three decades later very similar considerations have led to a revision of the Guidelines. Preparations for the review began in 2010 and the revised Guidelines were published in July 2013.

Background

The OECD has long recognized the important role of privacy as a fundamental value and a condition for the free flow of personal data across borders. In the early 1980s, approximately half of the OECD Member countries had passed or were about to pass privacy legislation. This triggered concerns that the risk of disparities in legislation would create obstacles to the free flow of information between countries. Given the international character of data flows it was felt that the issues could not be solved at national level but that an international solution was needed.

The Guidelines from 1980 contain the first internationally agreed upon set of privacy principles (approximately one third of the OECD’s Member countries being non-EEA countries). By following this principles-based approach and being drafted in a technologically neutral manner, the Guidelines have proved to be very flexible and adaptable to technological and societal changes. Although not legally binding, the 1980 Guidelines have influenced legislation and policy not only in the 34 OECD Member countries but also beyond. Today, its basic privacy principles are essentially reflected in all relevant general data protection frameworks worldwide.
AB EXTRA – THE OECD’S REVISED PRIVACY GUIDELINES

In essence, the eight basic data protection principles of the OECD Guidelines are as follows:

1) **Collection Limitation** – personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

2) **Data Quality** – personal data should be relevant, necessary, accurate, complete and up-to-date.

3) **Purpose Specification** – the purposes for the data use should in principle be specified at the time of the collection.

4) **Use Limitation** – personal data should in principle not be used for purposes other than those specified at the time of the collection, except in certain cases.

5) **Security Safeguards** – personal data should be protected by reasonable security safeguards.

6) **Openness** – data collection and processing should be transparent to the individuals.

7) **Individual Participation** – individuals should have the right to access personal data and have the data erased, rectified, completed or amended.

8) **Accountability** – a data controller should be accountable for complying with the implementing measures.

**Reasons for the review of the Guidelines**

Since the adoption of the Guidelines in 1980 the sheer volume of personal data has exploded. New technologies and processes have made personal data ubiquitous and globally accessible and innovative uses and analytics provide comprehensive insights into individuals’ movements, interests and activities. These developments have elevated the risks to individuals’ privacy, signaling the need for more effective safeguards. Moreover, privacy frameworks around the world are being examined and refined. Several initiatives have been undertaken to address the new challenges, such as the work on Binding Corporate Rules (“BCRs”) in the EU and the Asia Pacific Economic Cooperation’s Cross-Border Privacy Rules System. There is a proliferation of countries with data protection laws – some count more than 90 countries with data protection laws – and work on new privacy frameworks is underway, including in countries such as Brazil and China. These changes in personal data usage and the new approaches to privacy protection have triggered the review of the Guidelines.

**Impact on businesses**

Neither the 1980 Guidelines nor the revised Guidelines are legally binding for businesses and organizations or have any direct legal effect. However, companies are nonetheless well advised to study the revised Guidelines carefully and to prepare themselves for national legislation that is likely to be adopted as a result. The Guidelines represent a consensus by the most influential economies in the world on basic privacy principles and are intended to be used as a basis for new, or to be built into existing, data protection legislation. The 1980 Guidelines have been very influential and successfully trickled into most general privacy frameworks, including in countries that are not members of the OECD. It would therefore not come as a surprise if the same were to happen with respect to the revised Guidelines.

**Major changes in the revised Guidelines**

The eight basic privacy principles contained in the Guidelines were considered generally sound. Therefore, rather than fundamentally changing the Guidelines, the revised Guidelines introduce a number of new concepts, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness and global interoperability. They also update the 1980 Guidelines in several aspects, including accountability, transborder data flows and enforcement.

- **Privacy management programmes**

Privacy management programmes play an important role in the responsibility of organisations to protect personal data. In a new section on implementing accountability, the revised Guidelines introduce additional obligations on data controllers. In particular, they require data controllers to have in place (and to demonstrate as appropriate) a privacy management programme, giving effect to the aforementioned data protection principles.

The revised Guidelines spell out a number of essential elements of such programmes, such as safeguards based on privacy risk assessment, an internal governance structure, oversight mechanisms and incident response plans. The supplementary explanatory memorandum clarifies that such programmes should not only address the controller’s own operations, but also cover his employees or agents and even the relationship with other data controllers. Examples for safeguards listed in the explanatory memorandum include contractual provisions, including for sub-contracting, employee training and education as well as an audit process.
The revised Guidelines require controllers to notify significant security breaches affecting personal data to privacy enforcement or other authorities. Where the breach is likely to adversely affect individuals, the controller should inform these individuals.

Data flows

The revised Guidelines retain the approach that OECD Member countries should refrain from restricting transborder data flows among themselves where the other country substantially observes the Guidelines. But the revised Guidelines now put more emphasis on the accountability principle, which is explicitly restated in the context of transborder data flows.

More in particular, the revised Guidelines expressly recognise appropriate measures that controllers can implement and which, together with effective enforcement mechanisms, can qualify as sufficient safeguards. These safeguards are listed as the second scenario in which the Member countries should refrain from restricting transborder flows. This second scenario acknowledges safeguards put in place by controllers which are given quite some flexibility – they may achieve the required level of protection in different ways, including by a combination of different measures, such as security measures and audits.

Risk-based approach

The revised Guidelines adopt a more risk-based approach which is reflected in a number of changes to the 1980 Guidelines. Most notably, the Guidelines refer to the concepts of “risk” and “proportionality” in the context of transborder data flows and call upon Member countries to consider the sensitivity of data, the purpose and the context of the processing. The privacy management programmes should provide for appropriate safeguards based on privacy risk assessment. The revised Guidelines also recognise the importance of risk assessment in the development of policies and safeguards to protect privacy more generally. These changes will be welcomed by businesses as it allows for a certain flexibility and does not impose a “one size fits all”.

National privacy strategies and stronger enforcement

Businesses should also note that the revised Guidelines ask OECD Member countries to develop national privacy strategies, which should be complemented by education and awareness raising, skills development (including for privacy professionals) and the promotion of technical measures in particular with respect to privacy-respecting and privacy-enhancing technologies (also known as “PET”).

Businesses are also likely to face an increased enforcement risk in the future, including through joint enforcement action and investigations carried out by supervisory authorities. The revised Guidelines explicitly call for the creation of privacy enforcement authorities which must be equipped with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis. The explanatory Memorandum acknowledges the variety of possible mechanisms for this purpose.

A strong global network of privacy enforcement authorities is also seen as a first important step towards global interoperability. The revised Guidelines reiterate a commitment of the Member countries made in 2007 to enhance cooperation between privacy enforcement authorities.4

Impact on other privacy initiatives?

The Revised Guidelines were adopted at a time when the Council of Europe is continuing to debate the modernisation of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (the “Convention 108”) and the European Parliament and the Council (which is the EU institution representing the 28 Member States’ governments) discuss the reform of the EU Data Protection Directive.

Convention 108

The accountability principle as well as the issue of transborder flows also play a key role in the modernisation of Convention 108 which is currently being undertaken. Convention 108, adopted by the Council of Europe in 1981, is the first binding international instrument introducing principles for the protection of personal data. It has been ratified by 46 countries, the latest country being Uruguay as the first non-European country to accede.

Similarly to the OECD Guidelines, the review of Convention 108 has been triggered by the challenges for privacy resulting from the use of new information and communication technologies, the new realities of the online world and a much more globalised and interconnected world. The proposed amendments to Convention 108 are still being discussed by the Committee of Ministers, which set up an ad hoc committee on data protection to finalise the proposals.5
Several amendments to Convention 108 have been proposed to bring it more in line with the European Commission’s proposal for a General Data Protection Regulation (the “proposed GDPR”), published in January 2012. These elements include the accountability, privacy by design and privacy by default principles. Especially with respect to transborder data flows there are proposals to implement elements of accountability and to encourage the use of standard contractual clauses and BCRs. The proposed amendments also inject a risk-based element, according to the size of the controller, the volume or nature of data processed and the risks for the data subjects. The proposed amendments would pave the way for developing Convention 108 into a global data protection agreement.

As regards transborder flows, the proposed GDPR also introduces an element of accountability by officially recognizing BCRs as a data transfer mechanism. Other than the revised Guidelines, the proposed GDPR maintains the adequacy concept, requiring a detailed assessment of, among other things, the applicable laws and rules, but extending the concept to territories or processing sectors (in addition to countries as in the current EU Data Protection Directive).

The idea of a more risk-based approach as adopted in the proposed GDPR has been echoed by the Council, when examining the Commission’s proposal for the GDPR. In particular, the Irish Presidency has advanced amendments, trying to adjust the level of detail of some of the proposed obligations to the perceived level of risk.

Conclusion

Commissioner Reding would like to promote the proposed GDPR as the new gold standard of data protection. If adopted, the proposed GDPR will likely set a new and higher standard than the revised Guidelines or the (modernised) Convention 108. However, its success will depend, among other things, on how flexible an instrument it will be and how easily it can be adjusted to the fast-changing online environment.

Irrespective of the outcome of the legislative proceedings for the proposed GDPR and the modernisation of Convention 108 one thing is clear: the accountability principle and the transfer issue figure prominently in any debate on how to make privacy frameworks fit for the 21st century. They are crucial elements for the development of any sustainable framework in light of the globalisation and technological developments.

Monika Kuschewsky is Special Counsel at Covington & Burling LLP in Brussels. The views expressed in this article are personal to the author and do not reflect the view of Covington & Burling LLP or any of its clients.

mkuschewsky@cov.com

Footnotes

1 The OECD has done considerable work in the field of privacy. For example, projects have examined privacy notices and considered privacy in the context of horizontal issues such as Radio Frequency Identification (RFID). Current work is looking into privacy-related issues raised by Big Data use and analytics.

2 See the supplementary explanatory memorandum to the revised OECD Privacy Guidelines.

3 The basic concept of BCRe is that a group of companies undertakes to adhere to a set of internal binding rules for the intra-group transfer of personal data and to protect personal data accordingly.
