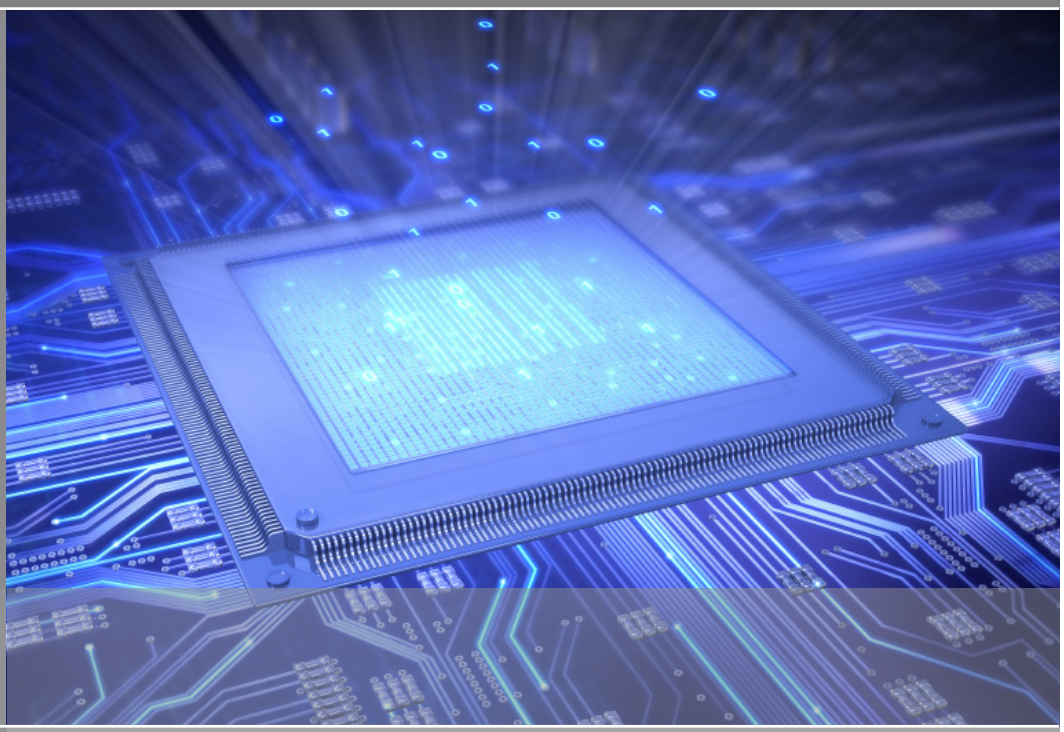
DATA TRANSFERS WITHIN A MULTINATIONAL GROUP

SAFELY NAVIGATING EU DATA PROTECTION RULES



Dechert LLP

MAY 2013

INTRODUCTION

Multinational corporations increasingly have a need to share their data throughout their group. Often this will be necessary to service international clients or to coordinate marketing efforts. Sometimes international data sharing will be necessary simply to implement a cost-effective centralised IT function. However, to do so often results in the group having to navigate the data protection or privacy laws of those countries in which they operate. A prominent example of an issue that arises is the European data protection restriction on transferring personal data outside of Europe (specifically, outside the European Economic Area (EEA)).[1]

This briefing introduces this issue and presents a summary of the solutions available to allow a transfer of data between group entities when some of the data crosses out of Europe. In particular, the following solutions are introduced:

- Ensuring that the recipient company is in a country automatically deemed adequate;
- Ensuring a US recipient is in the US "safe harbor" scheme;
- Putting in place certain types of data transfer contracts;
- Putting in place "binding corporate rules"; and
- (In the UK) undertaking a "self-assessment" as to the protection of the data throughout the group.

This discussion is focused on the responsibilities that entities based in Europe assume when they act as "data controllers" (the entity which determines the purpose for collecting the data). "Data controllers" are charged with ensuring that the personal data they collect is transferred in accord with EU and local laws. Different (albeit similar) considerations would apply if the European entity is transferring data which is controlled by a third party (for example, when a European service provider sends data controlled by that provider's customer).

DATA PROTECTION REFORM

Before reviewing the issues concerning the sharing of data within a multinational group, it is necessary to bear in mind that EU data protection is in the process of being reformed and that in undertaking any significant data protection compliance exercise it is sensible to have an eye on possible changes. The European Commission has proposed that the present scheme whereby a "Directive" has to be transposed into national law (with the possibility – indeed the reality – of different or even inconsistent requirements) will be replaced by a "Regulation". This would be directly effective within the member states and there will be no need for implementing domestic legislation.

A draft law has been prepared and inter-governmental discussions (with accompanying lobbying) are well under way. However, what is clear at this point is that the present draft of the Regulation preserves the main substance of data protection law as far as cross-border data flow issues are concerned. As an exception to this, the uniquely UK solution to the issue of "Self-assessment" which we discuss below would (on current proposals) be removed.

There are many other changes in the pipeline that are outside the scope of this briefing. Highlights include proposals for mandatory breach notification laws and enhanced powers for regulators to fine organisations for data protection non-compliance (up to a maximum of 2% of annual global revenues).

Whilst it is unclear what proposals will survive the scrutiny of the legislative process, nor what the timetable is for eventual adoption of the alternative rules, any compliance regime put in place now should put a group in a good position to prepare for increased data protection scrutiny within Europe for years to come.

DATA PROTECTION OVERVIEW

European data protection legislation governs the treatment of certain types of information, broadly, information about individuals, known as "personal data" in the legislation. These laws aim to impose minimum standards on those handling such information with a view to protecting the privacy of the individuals involved. It is inevitable, in most instances, that "personal data" will be involved when IT services are centralised or customer data is shared, for example, and these rules will be triggered.

The data protection law of each member of the EEA stems from the European Data Protection Directive (the Directive).[2] Each member has 'transposed' that

[1] The EEA is the European Union together with Iceland, Liechtenstein and Norway.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

directive into its national law. Therefore, in theory, there should be much commonality between the data protection regimes across the EU. However, as the member states have some discretion as to how to implement directives, there are 27 different implementations.

In any discussion on cross-border data flows it is important to bear in mind that European law contains a very wide definition of protected "personal data". This is any data 'which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'. Broadly, most businesses will, at a minimum, have information about their customers and suppliers and information about their employees. Emails inevitably contain personal data.

Data protection law in Europe distinguishes between the concepts of data 'controller' and data 'processor'. Broadly, the controller 'owns' the data, and the 'processor' is an agent handling the data for the controller. The individual to whom the data relates is referred to as a 'data subject' in the legislation.

A data controller has statutory responsibilities to data subjects and is subject to scrutiny of the regulatory regime and, ultimately, sanction through the courts; in most European jurisdictions, the processor has no such responsibility or real scrutiny.

THE TRANSFER RESTRICTION

Under Article 25 of the Directive personal data may not be transferred outside the EEA unless the data controller assures an 'adequate level of privacy protection', such transfers being subject to very limited exceptions. The rationale behind these rules, albeit perhaps difficult for non-Europeans to appreciate (especially when the laws of their countries are adjudged not to be 'adequate'), is logical: a data controller subject to the jurisdiction of the European rules and the safeguards imposed upon the personal data within Europe should not be able to send the data outside its borders without ensuring that an equivalent level of protection is afforded to a citizen's privacy. Otherwise the protection offered to the privacy of its citizens is severely limited as it would fall away by the controller simply sending the data abroad.

This restriction has proved problematic for many international businesses with a genuine need to share data throughout the world. It impacts upon the freedom to send data amongst members of an international group, or even simply from appointing an outsourced service provider outside of Europe.

COUNTRIES DEEMED AUTOMATICALLY ADEQUATE

The Directive allows the European Commission to make a finding in relation to the adequacy of the protection offered by a specific country. Transfers of personal data to the countries in this 'safe list' would automatically meet the adequacy standard. At the time of writing, only a small number of countries have been the subject of adequacy findings (including Argentina, Canada, Israel, Switzerland, Uruguay, Jersey, Guernsey and the Isle of Man).

THE US SAFE HARBOR

Introduction

The United States is not on the list of 'adequate' countries. This is an issue for US entities with either offices or affiliated entities based in Europe; these European entities and offices are considered "data controllers" under the Directive, and thus subject to its provisions. Many US companies in this position address this issue by signing up to a scheme called the 'Safe Harbor,' thus committing themselves to complying with a set of data protection principles.

There are seven principles, supported by guidance provided by the US Department of Commerce and a number of Frequently Asked Questions, that together broadly reflect the contents of the European rules. By complying with the Safe Harbor principles, US companies are deemed to have adopted an adequate level of protection for transfers of personal data to the US from EU member states. As such, if a US parent company, say, is a member for the relevant types of data, its European affiliates can transfer data to it without fear of contravening the transfer restriction.

The Mechanics of Safe Harbor

Joining Safe Harbor can be fairly straightforward. A US company would have to self-certify to the US Department of Commerce that it adheres to the Safe Harbor principles and make a public declaration of this adherence. Once accepted, a company is added to the publicly available Safe Harbor list.[3] Whilst

[3] Available through http://www.export.gov/safeharbor.

there is no approval mechanism (acceptance being a purely administrative act), a joining company should nonetheless ensure that its privacy policy is compatible with the principles and be prepared to make its privacy policy publicly available before going ahead with self-certification. A company has to verify annually the implementation of its privacy policy (this may be by self-verification or verification by a third party). It must also file a self-certification letter once a year.

US entities who wish to benefit from this scheme must take positive steps to comply with the seven principles.

How Are the Safe Harbor Principles Enforced?

The 'enforcement' principle of Safe Harbor (Principle 7) requires implementation by the joining entity of a suitable independent mechanism to deal with complaints or disputes and of a procedure for periodic verification of compliance with the principles. In addition, in relation to complaints, a company adopting Safe Harbor must either elect that a US self-regulatory organization is responsible for dealing with them or elect that such complaints fall under the jurisdiction of the European data protection authorities. Companies are committed to remedying complaints in accordance with their findings.

The Federal Trade Commission (FTC) and Department of Transportation (DOT) have the right to file deceptive trade practice charges against a company failing to live up to its Safe Harbor promises.

As well as regulatory enforcement, there is scope for both the transferring data controller (i.e., the European affiliate) and the individuals who form the subject of the transferred data, making a claim for damages in relation to a breach of the Safe Harbor principles. To date no such claim has been made.

Limitations on the Scope

Not all US entities are eligible to join. A fundamental requirement is that the entity is subject to the jurisdiction of either the FTC or the DOT (i.e., US air carriers and ticket agents). Two important sectors are not within that jurisdiction: the US financial services industry (regulated for privacy by the Federal Reserve and others) and telecommunications carriers (subject to the jurisdiction of the Federal Communications Commission).

STANDARD CLAUSES

Foreign companies which are located in countries outside the scope of automatically adequate countries and which are not US Safe Harborites can avoid the data export ban and receive data from their European affiliates by entering certain standard forms of contracts (known as 'standard clauses') with those affiliates. These will assure 'adequacy' for the purpose of the Directive.

There are two sets of standard clauses available for when the importer is a controller and one set for when the importer is a processor. To satisfy the regulatory requirement, each of the standard clauses must be used in the precise form approved.

It should be noted that there is a difference in approach to these contracts within Europe. Whilst they will always ensure "adequacy" for the purpose of the restriction, some European countries require the standard clauses (as executed) to be filed and even approved prior to the initial transfer. Other countries, such as the UK, require no additional formality.

There are some points to note with this solution. The standard clauses are contracts and can therefore be enforced both by the exporting group entity (perhaps not a real risk) and by the data subjects who are expressly given "third party beneficiary" rights in the contracts to enforce at least some of the terms in certain circumstances.

BINDING CORPORATE RULES

A further method of legitimizing transfers of data outside of Europe is by having a set of so-called 'binding corporate rules' (the BCRs) approved by the European regulators. These facilitate the international sharing of data between entities within the same group.

The scheme involves the corporate group setting up an internal suite of documents setting out how the group intends to provide adequate safeguards to individuals whose personal data is being transferred to a third country. These must contain data protection safeguards no less than those provided for in the Directive. Setting BCRs can be a challenge because a corporate group must create legally-binding internal documents for the benefit of affected individuals, with one delegated company taking responsibility for the compliance of the whole of the group while the rest of the group is required to undertake comprehensive data protection audits. When all these internal

steps are completed, the BCRs are submitted to one national data protection regulator (perhaps in the country where the organization has its EU headquarters).

The rules now contain a mutual recognition process applicable to most (but not all) member states.[4] Under the scheme, if one of the member countries, taking on the role of the lead authority, approves an application for BCRs, the BCR is automatically approved in the other member countries.

Not surprisingly, BCRs have been criticized as offering a solution that is only really appropriate for the most sophisticated international organizations. After an unimpressive start, BCRs have recently gained some momentum in the wake of standard 'checklists' and processes, and the mutual recognition schemes. Since then large multinational companies such as Accenture, Atmel and Hyatt have opted for BCRs as their regime of choice for complying with the Directive.

BCRs may be appropriate where many countries outside of Europe are involved as recipients or where the group is in a constant state of flux. In those circumstances, the substantial upfront investment in putting BCRs in place will create compliance and administration savings down the road. However, if there are only a handful of non-European destination countries for the data, it may be easier simply to put in place standard contracts.

SELF-ASSESSMENT

The 'self-assessment' approach to legitimizing transfers of data from member states to third countries is a valid approach in the UK, but not generally throughout the other member states. The approach is based on the premise that the data exporter should itself consider and make a judgement as to whether, in the particular circumstances of a transfer, that transfer is made to a country that can ensure an adequate level of protection. The UK Data Protection Act 1998 imposes a direct obligation upon data controllers to ensure, and assess, adequacy of the protection of the data when it is transferred.

This compliance method can certainly be useful in arrangements such as those covered in this note where a UK affiliate wishes to share data with its US affiliates. The approach has been endorsed by the UK Information Commissioner's Office (ICO) generally although the ICO would expect – on any enquiry – that the controller can demonstrate that an appropriate analysis has been undertaken.

The UK ICO's guidance on data transfers emphasizes that when a controller is considering whether there is an adequate level of protection it should take into account a number of factors. These include certain specific criteria related to the data itself such as the nature of the personal data, the purposes for which, and period during which, the data are to be processed, and any security measures to be taken. However, there is also a requirement to consider more general 'legal adequacy' factors in the destination country. Here a controller should consider the background legal provisions in force in that country that will give protection to the data (even if not in the same way as in Europe), including any relevant codes of conducts and treaty obligations. Having said that, the UK ICO recognizes that it would be inappropriate for exporting controllers to consider such legal adequacy criteria exhaustively in the case of every transfer to a third country. Nonetheless, controllers are expected to be able to recognize countries where there would be a real danger of prejudice or where it is clear that the country in question does not provide any legal protection in relation to the exported data.

Where the transfers to a non-EU group entity is because of the centralisation of IT resource (such as centralised Email servers), then that is arguably tantamount to an outsourcing (although an intra-group one). In relation to outsourcings generally, the ICO makes it clear in its guidance[5] that the transfer would not normally present a problem from the perspective of the transfer restriction and that the parties do not, in fact, ordinarily have to put in place standard clauses. In its guidance, provided it has properly dealt with its security responsibilities (including flowing down those responsibilities to its contractors).

CONSENT AND OTHER DEROGATIONS

There are other methods of transferring personal data to third countries. A transfer can take place without a need to worry about one of the methods just

[4] Including France, Germany, Ireland and the United Kingdom.

[5] This guidance comprises two separate documents: a legal analysis of the eighth principle entitled 'The Eighth Data Protection Principle and international data transfers' (the UK Legal Analysis) and also a more business orientated paper containing general compliance advice for companies transferring personal data overseas (the UK General Compliance Advice).

discussed if, for example, the transfer is necessary for the performance of certain contracts, or if there are important public interest grounds, or a need to establish, exercise or defend legal claims.

Consent is often discussed in this context but it is not without problems (a full discussion of which is outside the scope of this note). Whilst it is superficially attractive, consent must be given freely, be specific and informed and, where sensitive personal data is concerned, must also be 'explicit'. Further, difficulties would arise in collecting consents from a large number of individuals: what if one of many withholds consent? What if one data subject revokes their consent?

PRE-IMPLEMENTATION COMPLIANCE HOUSE-KEEPING

Whatever solution a group puts in place, there is likely (in some jurisdictions, if not all) to be a need to make a filing with the local regulator. As a result of any filing relating to the transfer, it is possible that there will be greater scrutiny of general data protection compliance by the local regulator.

As such, it is prudent to first carry out a general health-check of compliance with local requirements of notification and registration with data protection authorities. The group bringing itself into compliance on the transfer issue does not want to notify (or negotiate a BCR) when a "base" registration that might be needed independently of the transfer is not yet in place.

CONCLUDING REMARKS

Data transfers cause much concern within organisations operating internationally and within Europe, especially with the increasing scrutiny of privacy rules, and the increasing powers of regulators to levy financial penalties. If the enhanced powers of fines suggested by the European Commission for data protection breaches in the proposed Regulation (of up to 2% of global revenue) survives the legislative process this is only likely to increase. The issue is capable of resolution and for most organisations the best choice among the various solutions will become apparent when a survey of the data flows is undertaken.

A more detailed version of this briefing is available on request from Renzo Marchini, the author, or from your usual Dechert contact.

Renzo Marchini
London
+44 20 7184 7563
renzo.marchini@dechert.com

PRIVACY AND DATA PROTECTION AT DECHERT

Dechert's Privacy and Data Protection lawyers assist clients in complying with the many, and often inconsistent, rules and regulations established to protect the privacy of customer and employee information, working to minimize the cost and time for compliance. We have particular expertise advising clients around the world on privacy and data protection in the financial services, consumer marketing, healthcare and life sciences sectors.

PRIVACY AND DATA PROTECTION GROUP: KEY EUROPEAN CONTACTS

Dr. Olaf Fasshauer
Munich
+49 89 21 21 63 28
olaf.fasshauer@dechert.com

Jonathan A. Schur
New York
+1 212 698 3552
jonathan.schur@dechert.com

Renzo Marchini
London
+44 20 7184 7563
renzo.marchini@dechert.com

Marianne Schaffner
Paris
+33 1 57 57 80 60
marianne.schaffner@dechert.com

Dechert is a global specialist law firm.

Focused on sectors with the greatest complexities, legal intricacies and highest regulatory demands, we excel in delivering practical commercial judgment and deep legal expertise for high-stakes matters.

In an increasingly challenging environment, clients look to us to serve them in ways that are faster, sharper and leaner without compromising excellence.

We are relentless in serving our clients – delivering the best of the Firm to them with entrepreneurial energy and seamless collaboration in a way that is distinctively Dechert.

dechert.com

Almaty • Austin • Beijing • Boston • Brussels • Charlotte • Chicago • Dubai • Dublin • Frankfurt • Hartford
Hong Kong • London • Los Angeles • Luxembourg • Moscow • Munich • New York • Orange County • Paris
Philadelphia • Princeton • San Francisco • Silicon Valley • Tbilisi • Washington, D.C.

Dechert LLP