ALLEN & OVERY

September 2015

EU data privacy challenges in responding to data requests made by U.S. authorities

Nigel Parker, Partner

Context

Regulators, courts and law enforcement authorities in the U.S. (and other jurisdictions around the globe) have an insatiable appetite for access to data held by a range of companies, including in particular financial institutions, telecoms operators, online retailers, cloud providers and other internet service providers.

The data requested often includes personal data (also known as personally identifiable information), which may comprise data relating to employees, clients or other individuals connected with a business.

Complying with any given request will require a company with operations in the EU to navigate various restrictions, which may include EU data protection and privacy laws, duties of confidentiality arising at law, contractual restrictions, or in some cases specific blocking legislation (eg in France).

The conflict is not just technical in nature; it partly reflects a cultural difference between jurisdictions, particularly between the EU and U.S., and also a difference between the objectives and priorities of sectoral regulators and law enforcement authorities, in one corner, and data protection authorities in the other.

Some companies have recently been involved in high-profile attempts to resist demands from law enforcement authorities for access to data they hold about their customers. Most notably, Microsoft is in the process of appealing a decision of a New York District Court, which held it in contempt for failing to comply with a demand that was served by federal agents on Microsoft's U.S. headquarters requiring it to hand over data about EU customers held on servers in Dublin, Ireland. Microsoft apparently receives tens of thousands of law enforcement requests each year.

Post-Snowden, governments (especially in the EU but also in China and elsewhere) have expressed unease with the long arm of U.S. authorities, and are increasingly taking action to resist the exercise of extraterritorial jurisdiction by U.S. courts and law enforcement authorities. This has led, for example, to the proposed EU General Data Protection Regulation (in certain versions of its current draft form) specifically prohibiting the sharing of personal data with foreign authorities other than with the specific prior approval of a domestic data protection authority, punishable by potential fines of up to 5% of turnover. And it has led to some EU Member States withdrawing their support for reliance on the U.S. Safe Harbour scheme in data protection law, pursuant to which many companies undertake data transfers to the U.S., as well as efforts by the European Commission to renegotiate the terms of that scheme to ensure the better protection of data.

The conflicts of law presented by requests for data by foreign authorities are a significant problem for many businesses – especially those with significant U.S. operations or which are headquartered in the U.S.

The recently announced EU-US umbrella agreement for cooperation between law enforcement authorities, in the context of preventing, investigating, detecting or prosecuting criminal offences, will only allay these differences in the context of police cooperation and judicial cooperation in criminal matters (ie not in relation to transfers by private companies in the EU to US authorities).

Here we examine the nature of the conflicts which arise as a result of data protection restrictions, some strategies to navigate those restrictions, including practical recommendations on how best to prepare for a request and how to respond when a request is received.

EU data protection restrictions

The European Data Protection Directive 95/46/EC (the **Directive**) sets out a number of general rules in relation to the lawfulness of the processing of personal data and criteria for making data processing legitimate.

In relation to requests received from authorities, the key relevant rules and criteria are:

- the principle that certain criteria for making processing legitimate (known in the UK as "fair processing conditions") must be satisfied (a ***legitimacy*** requirement)
- the requirement that information must be provided to the data subject about the purposes of processing for which data are intended (a ***transparency*** requirement)
- specifically in relation to requests from outside the EEA, the requirement that data should not be transferred to a third country unless that country ensures an adequate level of protection (a ***cross-border transfer restriction***).

Typically, it will be possible to disclose data in compliance with national laws implementing the Directive where a request is made by a domestic regulator, court or law enforcement authority from within the relevant EU Member State, although it is still important that each request be considered on a case by case basis. This is because domestic requests will - having the compulsion of law or on the basis of some national public interest - in most circumstances satisfy the criteria for making processing legitimate, and because there will usually be an available exemption in relation to the transparency requirements.

However, where a request is received from a U.S. or other foreign regulator, court or law enforcement authority, it is often not possible to transfer data without breaching national laws of EU Member States which implement the provisions of the Directive. This is because the existence of a compulsion of foreign law or a foreign public interest does not by default establish legitimacy, such that it would enable a company contemplating disclosure to satisfy one of the criteria for making processing legitimate. Further, it may not be possible to fall within the narrowly construed exemptions to the transparency requirements or derogations to the restrictions on cross-border transfers outside the EEA. It is important, however, to consider the particular context in which each request is received against the relevant rules. As with requests originating within the EU, there may be steps that can be taken to legitimise the disclosure or transfer of personal data where it is necessary to comply with a request by a U.S. regulator, court or law enforcement authority.

Enforcement risk

Compliance with a request for personal data from any sort of authority could cause a company to breach EU data protection and other laws as implemented in individual EU Member States.

Companies can therefore find themselves between a rock and a hard place, faced, in many cases, with the reality of potential sanctions against them regardless of how they act. The risks and sanctions under national laws implementing the Directive therefore needs to be weighed against the risks and potential sanctions that could result from failure to comply with a request.

A failure to comply with the laws implementing the Directive is unlikely to amount to a criminal offence, except in rare cases (eg in France, where a breach of the blocking statute is a criminal offence). However, data protection authorities may take enforcement action in respect of a breach, which may result in fines and other sanctions.

The data protection authority may also seek public undertakings from a company, which may "name and

shame" offending companies, which can in turn cause damage to a company's reputation.

Last, and by no means least, a data subject who suffers damage or distress may have a right to seek compensation from a company which discloses their data.

Practical recommendations

The net effect of the restrictions described above is that EU data protection laws can put companies in a position where it is often not possible to comply with requests without breaching the legal barriers that exist. In particular:

- There is often no general exemption that can be relied on or action that can be taken to overcome the restrictions. Specifically, compulsion of foreign law or courts never provides an exemption in itself. If it did, it would effectively allow foreign authorities to circumvent EU law.
- Exemptions that do exist are construed narrowly. Further, as a practical matter, consents from data subjects that might legitimise transfers are often not in place on a consistent basis to enable information-sharing with authorities.
- Where compliant means of responding are available, such as through mutual legal assistance treaties, for instance the Hague Convention, they are often not used by the requesting authorities (eg because they slow things down, or because of a requirement for dual criminality between the requesting jurisdiction and the jurisdiction where data is located).

We have set out below some practical recommendations on possible steps that can be taken in anticipation of, and to respond to, requests.

Recommended steps to take before receipt of a request

(1) **Minimisation/retention policy** – only retain information which is required for business or regulatory reasons. Retaining data can be expensive, and may be inconsistent with data protection laws, but it also exposes the company to additional cost and risk in the event of a request. Companies should implement retention and destruction policies which ensure that only necessary information is retained.

(2) **Standard notice and consent** – standard form notice and consent language included in customer and employee terms and conditions should address transfers to domestic and foreign regulators, courts and law enforcement authorities. It should address transfers not just for the purposes of compliance with law, but also compliance with other requests which may not involve compulsion of law on the company.

(3) **Model clauses/binding corporate rules** – companies should implement a framework to allow for intra-group transfers of personal data. This may take the form of model clauses or binding corporate rules. This will allow intra-group transfers, which may be a precursor to a transfer pursuant to a request. For example, a company may wish to undertake an internal review of relevant information in a foreign jurisdiction before disclosing information pursuant to a request.

(4) **Policy** – companies should implement policies to ensure requests are properly considered and that a consistent approach is taken as far as possible. This will demonstrate to the data protection authorities that the company has considered its obligations under the laws implementing the Directive. The policy might distinguish between different processes depending on the data, source and destination country and other factors.

Recommended steps to take on receipt of a request

(1) **Legal powers** – consider whether there is actually a legal obligation to respond to the request and, if so, to what extent. Regulators and law enforcement authorities in particular will often request information where there is no legal power to compel disclosure of that information, or they will not follow the correct procedures to make a binding demand for information. It is important to examine the nature of the request, as it could determine whether or not a disclosure or transfer is within the scope of any consent given by the data subject or derogations. It may be appropriate to revert to ask the regulator or law enforcement authority to make a binding request.

(2) **Seek further information** – it is advisable to seek further information in writing from the requesting regulatory authority, to evaluate what the purpose of the request is. It is important to examine the purpose of the request, as it could determine whether or not a disclosure or transfer is within the scope of any consent given by the data subject or derogations under the Directive.

(3) **Negotiate scope** – it may be advisable to negotiate the scope of the request, as in some cases regulators or law enforcement authorities will agree to narrow broadly defined requests to target specific information that is required for the purposes of their investigations. This will save cost and reduce risk, but needs to be balanced against the need to maintain a good relationship with the requesting regulators and law enforcement authorities.

(4) **Data minimisation or anonymisation** – companies should always limit the data disclosed and transferred to that which is necessary for the purpose. This may involve undertaking an internal review process, possibly with the assistance of external advisors. If the requesting regulator or authority does not require personal data, it may be possible to redact certain personal or other sensitive information from documents before they are transferred and/or disclosed. If so, this will allow a company to reduce risk, although it will result in additional costs in connection with the review and redaction process.

(5) **Consider obtaining consent and/or giving notice** – in some cases, it will be possible to obtain a specific consent from individuals to undertake a particular disclosure and transfer. Where this is possible, eg where the number of individuals is small and they are cooperative, this may be a useful additional means to legitimise the transfer and/or disclosure. However, equally, relying on consent as the only basis for legitimising transfers is not generally recommended.

(6) **Data processing agreement** – if transferring data to an affiliate or a third party as an interim measure, and that affiliate or third party will be acting as a data processor, it is necessary to put in place a data processing agreement, under which the data processor is required only to process data in accordance with the instructions of the company (as data controller), and to implement sufficient technical and organisational security measures to protect the personal data.

(7) **Consider transfer via domestic authority** – in certain cases, it may be possible to request that the requesting regulator requests data via a domestic regulator of the company. This may be possible where the two regulators have entered into a memorandum of understanding or similar concerning international cooperation (eg such an agreement exists between the SEC and the FCA). Alternatively, foreign authorities can request that a domestic court compel the disclosure of documents pursuant to the Hague Convention, although this process is not often used in practice due to the obstacles to and expense of going through that process.

Allen & Overy LLP

One Bishops Square, London E1 6AD United Kingdom | Tel +44 (0)20 3088 0000 | Fax +44 (0)20 3088 0088 | www.allenovery.com