

Article 29 DP WP on transborder discovery rules and EU DP laws

Companies ought to review or establish e-discovery policies and procedures. A country-by-country approach needs to be adopted due to differing national laws. **Gary Brooks** reports.

Imagine you are the Privacy Officer of a multinational organisation that receives a request from a US court for the production of personal data which is stored on the server of a European affiliate – you are faced with a dilemma: satisfy compulsory US discovery obligations or instead comply with European data protection laws, which can restrict data disclosures for litigation purposes. There are potentially serious consequences of failing to comply with either legal regime.

The Article 29 Data Protection Working Party (Art. 29 DPWP) – the group of national Data Protection Commissioners on 11 February adopted its long-awaited Working Document on “pre-trial discovery for cross border civil litigation”¹. The WP expressly recognises the need for reconciling the requirements of US litigation rules and EU data protection laws and provides guidelines for businesses on how to manage this conflict in practice.

This is an emerging and difficult problem, particularly for European affiliates of a multinational company. This article considers the nature of the problem, explains the legal issues in the EU Data Protection Directive² (“the Directive”) governing e-discovery requests, examines the WP guidance and then sets out some further practical steps which organisations can take to tackle the issue.

Scope of the Working Party Opinion

A large part of the WP paper summarises the differing legal regimes in various countries concerning pre-trial discovery, but it focuses on the US litigation rules which are most frequently encountered in practice. The paper assesses the handling of litigation in two different areas; pre-emptive document preservation and pre-trial discovery requests.

1. Document preservation

The US Federal Rules of Civil Procedure (namely Rules 26 and 34), impose broad obligations on US companies involved in litigation, which are notably wider than the equivalent rules in EU jurisdictions. Rule 34 requires the company to retain/preserve all documents (including both paper and electronic files) which may be relevant to actual or reasonably foreseeable litigation, and crucially, the duty applies wherever in the world such documents are located.

2. Pre-trial discovery requests

Rule 26 states that all parties in litigation must disclose “a copy of, or description by category and location of, all documents, data compilations and tangible things in possession, custody or control of the party that are relevant to disputed facts alleged with particularity in the pleadings”.

Having received an e-discovery request, the process of retaining, identifying, reviewing and transferring documents that are relevant to the litigation will amount to “processing” of personal data and so will be subject to European data protection laws, where the documents are held in the EU and to the extent they contain information about identifiable individuals. This personal data will typically relate to the organisation’s employees or third parties, such as clients or customers.

There are potentially serious consequences for not complying with US discovery obligations. These include criminal sanctions (such as fines) and the possibility that the US Court can issue an “adverse inference instruction” to the jury, allowing them to draw the inference that the evidence may have been adverse to that party if they had produced it.

The consequences of not complying with European data protection laws include disruptive and costly investiga-

tions from the data protection regulator (and the resulting adverse publicity), enforcement action (which may include fines) and potentially compensation claims from the individuals concerned if they suffer a loss.

Blocking statutes and other applicable national EU laws

As well as data protection laws, the WP paper points to an additional obstacle in certain EU countries (for example France) where so-called “blocking statutes” explicitly prohibit the cross-border discovery of information that could be used in connection with a foreign legal proceeding. Indeed in 2008, the French Supreme Court upheld the conviction of a French lawyer who had complied with a discovery request from a US court, in breach of the French statute³.

Complying with an e-discovery request is likely to require access to an employee’s e-mail folders (amongst other internal documents). Whilst not mentioned in the WP paper, in addition to data protection law requirements, there may also be local labour or constitutional laws which have to be considered, since they may restrict or prohibit review of employee e-mail folders. For example in Greece, accessing employee e-mails without prior notice and without allowing the individual the opportunity to protect the secrecy of his communications is illegal and can be criminally prosecuted. These differing national laws present real practical difficulties and require a country-by-country assessment to be adopted.

Working Party guidance for data controllers

While the WP guidelines are not binding, they lay the foundations for practical solutions to be developed and they are likely to be taken into account by national data protection authorities

in the EU when assessing whether a European company has breached national law by complying with an overseas discovery request.

The paper helpfully focuses on each of the four stages of the litigation process which result in data being processed beyond the scope of what the parties originally intended: retention; disclosure; onward transfer; and secondary use. The four activities each amount to “processing” of personal data and will require an appropriate fair processing condition to be met in order to legitimise such uses of data.

On the first issue of retention, the paper points out that European businesses have no legal basis under EU data protection laws for storing personal data for an indefinite period because of the possibility of litigation in a foreign jurisdiction, however remote this may be. A useful practical tip is provided: the US rules on civil procedure only require the disclosure of existing information, so if the European business operates a data retention policy with short retention periods in order to comply with local data protection laws, it will not be found at fault with US law if it no longer holds the data that is subject of a request received from a US Court.

Whilst all the EU data protection obligations potentially apply to the use and disclosure of personal information for litigation purposes, the following are the most important: Fair processing, purpose limitation, international data transfers.

Articles 7 and 10: fair processing

In order for the pre-trial discovery process to take place lawfully, the processing of personal data needs to be legitimate so as to comply with Articles 7 and 10 of the Directive. In particular, the business must:

1. inform the individual of the litigation purposes for which his/her data is being retained/disclosed and the identity of the recipients; and
2. meet a fair processing condition to legitimise the retention and disclosure of personal data for litigation purposes.

As far as the transparency obligation (1 above) is concerned, the paper points out that whilst this is perhaps

the most important of all the data protection requirements, there is a limited exception to the rule in cases where there is a substantial risk that notifying individuals would jeopardise the ability of the litigating party to investigate the case properly or gather the necessary evidence.

As for the latter requirement to meet a fair processing condition (2 above), the Art 29 DPWP identifies three relevant grounds in the Directive that would legitimise processing of data for pre-trial purposes:

- consent of the data subject,
- compliance with a legal obligation, or
- further processing based on a “legitimate interest” pursued by the data controller or by the third party to whom the data are disclosed.

Consent

The WP’s views on the limitations of consent (as published in previous WP Opinions) is again evident in this context of litigation, with the WP stating that it is “unlikely that in most cases consent would provide a good basis for processing.” Consent by an individual in this context to data processing for litigation purposes is unlikely to be regarded as freely given and therefore valid. A valid consent also implies that individuals should be able to withdraw their consent without suffering any consequences, which is not possible in the context of discovery.

Necessary for compliance with a legal obligation

One of the most significant aspects of the WP paper is that it makes clear that EU business cannot, in order to legitimise data processing activities relating to foreign discovery requests, rely on the ground which allows for personal data to be processed where it is “necessary for compliance with a legal obligation⁴”. An obligation imposed by a foreign legal statute or Court will not qualify as a legal obligation for the purposes of this condition⁵. However, if it is a requirement of the national laws of the EU country to comply with an Order of a Court in another jurisdiction seeking discovery, then clearly the business can rely on this condition to justify the processing of personal data in order to comply with the request.

Necessary for the purposes of a legitimate interest

In the absence of a valid and freely given consent from the individuals concerned, the “legitimate interests” condition is the most likely to provide a valid basis for processing data pursuant to litigation demands.

The WP recognises that parties involved in litigation have a legitimate interest in retaining, accessing and disclosing information that is necessary to make or defend a claim. But in order to rely on this ground, it is necessary to balance this interest with the privacy rights of the individual whose personal data is sought.

This balance of interest test should be applied on a case-by-case basis and involves taking into account the relevance of the personal data to the litigation and the consequences for the individual of processing the data.

Purpose limitation and proportionality

Under Article 6, personal data must be “collected for specified, explicit and legitimate purposes and not used for incompatible purposes.” Personal data must also be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.”

The WP states that compliance with these principles may require filtering of personal data while still in Europe to limit the data to that which is “objectively relevant to the issues being litigated”, and this filtering process may require “the services of a trusted third party in a Member State.”

International data transfers

Article 25 of the Directive provides that the transfer of personal data to a country outside the European Economic Area may take place only if such a country ensures an “adequate” level of data protection. The European Commission has designated a number of countries as providing adequate protection but the US is not on the list of approved countries.

Transfers of personal data to the US therefore require a legal basis and the Directive provides exceptions to the data exports restriction including in circumstances where the transfer is “necessary or legally required for the

establishment, exercise or defence of legal claims". There may be scope to rely on this condition to justify a single transfer of all relevant information to the US for discovery purposes, but the WP paper points out that this particular derogation has been interpreted narrowly by the European regulators.

If a significant amount of data is being transferred to the US, the WP identifies three main grounds which will allow transfers to occur where the recipient:

- is established in the US and has subscribed to the EU/US Safe Harbor scheme; or
- has entered into a data transfer contract with the data exporter (for example, based on the European

Commission's Standard Contractual Clauses); or

- has put in place Binding Corporate Rules (BCR) for its cross-border data flows (this is unlikely to be applicable in practice, given that at present very few companies have successfully adopted BCR).

Compliance with a discovery request made under the Hague Convention⁶ would also provide a formal basis for a transfer of personal data to the US and the WP encourages litigating parties to use the Convention wherever possible.

Conclusion

The WP Opinion is to be welcomed in that it adopts a moderate and pragmatic

approach to the issue (by recognising US discovery goals as legitimate) and it provides useful guidance in identifying the main data protection compliance issues and advising on how best to facilitate compliance with US discovery obligations whilst complying with the Directive. Not only do the European regulators expressly recognise the dilemma faced by businesses in reconciling this conflict of laws, but they also seem committed to finding a workable solution.

However, it is fair to say that aspects of previous WP opinions are simply repeated in this paper and the guidance doesn't tell data controllers grappling with this problem much that is particularly new. Nevertheless, the

PRACTICAL MEASURES TO MINIMISE DATA PROTECTION RISK

The challenge for European businesses is to take the broad principles set out in the WP opinion and convert them into practical measures to manage these foreign e-discovery requests and to reduce the risk of breaching EU data protection laws in the event that the decision is made to comply with the request.

There are a number of steps which can be adopted as follows:

1. Establish or review discovery policies and procedures

What is your organisation's discovery policy for managing e-discovery requests and conflicts with EU data protection laws? This policy should be reviewed (or established!) in light of the WP guidance and consideration should be given to the practical areas set out in sections 2 and 3 below.

2. Plan ahead with compliance strategies

Consideration should be given to adopting the following measures, which will assist in resolving the cross-border compliance challenges when faced with a subsequent e-discovery request:

- Ensure that all relevant Privacy notices address the use and disclosure of personal data for the purposes of litigation/investigations.
- Ensure that employee monitoring/IT acceptable use policies cover the review of employee e-mail and other personal data for litigation and investigation purposes.
- Consider where your personal data is currently held, with a view to centralising data storage in one jurisdiction.

- The applicable data protection law in the EU is the law of the Member State where the personal data (that is the subject of the e-discovery request) is held. It may be desirable to manage e-discovery requests for European data from the UK as far as is possible (for example by storing all personal data that is likely to be subject to foreign discovery requests in a central database managed in the UK). Whilst desirable, this may well be impossible to achieve in practice.
- The advantage of being subject to the UK data protection regime when disclosing personal data in response to a foreign discovery request is that the UK Information Commissioner adopts a more moderate and pragmatic approach to the interpretation and enforcement of the data protection legislation than many of his European counterparts. In addition, the UK does not have any blocking statutes.
- Ensure that EU affiliates' data protection registrations refer to processing of personal data for litigation and investigation purposes.

3. Establish process for managing discovery requests

A country-by-country approach should be adopted due to differing national laws, and it is necessary to look at all the circumstances of each case before deciding whether personal data can be retained or disclosed in pursuance to a particular preservation order or discovery request. The following measures should be considered once an e-discovery request has been received:

- Identify the information that is relevant to the case and plan ahead in order to narrow the range of records that have to be reviewed and produced.
- If the individuals' identity is not relevant to the cause of action in the litigation, anonymise their personal data where possible (for example by removing their names) prior to disclosure.
- Examine the local data protection law in detail – are there any exemptions which may be applicable to allow the disclosure? Are there any other national laws or blocking statutes which have to be considered? On the flipside, what are the consequences of not complying fully with the discovery request?
- Where data disclosure is to occur, ensure that notification is given in a timely fashion to affected individuals of the nature and extent of the data processing for litigation purposes (and details of any privacy safeguards which the organisation has put in place)
- Consider applying to the US courts for a "protective order" against the recipient of the personal data, which clarifies EU data protection requirements, requires measures to minimise information collection and dissemination, and specifies procedures for safeguarding information security and for deleting the data once the litigation is finished. The WP suggests that a protective order could impose obligations on the recipient to comply also with individuals' right of access, rectification and erasure (as enshrined in the Directive)

MANAGEMENT/NEWS

document recognises its limitations and states that it is an “initial consideration” of the issue and forms an invitation to public consultation with the Working Party – an invitation which will be of interest to many multinational businesses.

The WP Opinion rightly states that an inter-governmental solution is the only long term solution to this conflict. This is not just a European privacy problem however, since e-discovery/privacy conflicts could also affect other countries with data protection laws based on the EU model, such as Argentina, Canada, Israel and Dubai. Any agreement should therefore be global in nature and the WP opinion is best viewed as the first step on a long road towards that goal.

REFERENCES

1. WP 158 (Working Document 1/2009 on pre-trial discovery for cross border civil litigation)
2. Directive 95/46/EC
3. *Strauss v Credit Lyonnais S.A.*, 2000 4. US Dist. Lexis 38378
4. Article 7 (c) of the Directive
5. This is consistent with a previous Article 29 WP Opinion on whistleblowing schemes, which reached the same conclusion (See WP 117).
6. The Hague Convention provides a stan-

dard procedure for issuing “letters of request” or “letters rogatory” which are petitions from the court of one country to the designated central authority of another requesting assistance from that authority in obtaining relevant information located within its borders. Not all EU Member States are parties to the Convention however and many signatory States have effectively signed with reservations, so this limits its scope of application, in practice.

In the meantime, all businesses can do is devise practical methods of minimising the risks of breaching EU data protection laws when dealing with e-discovery requests.

INFORMATION

Gary Brooks is a data protection consultant to *Privacy Laws & Business* and to others, including law firm Berwin Leighton Paisner
E-mail: gary@dataprotected.co.uk
www.dataprotected.co.uk