Electronic Discovery Products and Services

WHITE PAPER

Privacy considerations affecting data required for litigation and regulatory purposes

by

Chris Dale of the
UK e-Disclosure Information Project

in association with

OutIndex

Chris Dale | e-Disclosure Information Project | **T:** +44 1865 463033 | **M:**+44 7770 580640
chrisdale@chrisdalelawyersupport.co.uk | www.chrisdalelawyersupport.co.uk

1 Introduction

Companies doing business in both the US and the EU are increasingly aware of the conflict between EU data privacy laws and the requirements of US courts and regulators. The latter claim rights of investigation over any world-wide branch of a company within its own jurisdiction. The EU exerts rigorous control over the use, and particularly the export, of personal data. The US demands are frequently wide in scope and short in timescale. The EU requirements are detailed in effect and do not lend themselves to quick solutions. There is an obvious conflict.

1.1 OutIndex

OutIndex specialises in data processing both by developing software for sale to others and through its own data collection and processing services. Unusually for such a business, it originated in the UK and expanded to the US, with offices and data processing facilities – and experience – in both continents and under both sets of court and regulatory regimes.

1.2 The e-Disclosure Information Project

The e-Disclosure Information Project is run by Chris Dale, a former litigation solicitor and software developer, to do what its name implies – to bring information and awareness to lawyers, courts, corporates and suppliers as to the law and practice of electronic disclosure in the UK, informed by strong links with US and Australian experts.

1.3 Purpose of the White Paper

This White Paper aims to give a high-level overview of the problems which can arise from the collision between the conflicting demands outlined above. These are rarely insuperable, but overcoming them requires a mixture of practical, legal and cultural inputs and, ideally, some pre-planning.

This paper is for informational purposes only and does not purport to be or to include legal advice. You should take appropriate advice before engaging in any activity referred to in this paper.

2 The Legislative Context

2.1 The Directive 1995/46/EU

The source of the EU privacy rules is the EU Data Privacy Directive 1995/46/EU which requires member states to pass data protection laws covering the *personal data* of or about *data subjects*. *Personal data* is widely defined – it covers any information relating to an identified or identifiable natural person. There are certain "special categories" of data relating to racial or ethnic origin, political and religious beliefs, health and sex life. The identification of these as "special" does not derogate from the restrictions on wider matters.

Each member state makes it own laws. France and Germany have particularly strong protection, especially in respect of workplace privacy. Data controllers who send data outside the EU in breach of the restrictions can be punished personally. Whilst this has hitherto been a rare occurrence, it has happened e.g. in Finland.

2.2 Transfer of data outside the EU

The Directive and the national laws to which it is parent would be easily circumvented if EU companies could simply send it outside the EU for processing in more benign regions. It can only be sent to a handful of countries which are recognised as having an adequate level of protection in their own privacy laws. Canada is one of these countries. The US is not.

The commercial difficulties which this caused led to high-level discussions between the EU Commission and US Department of Commerce. These have led to some relaxation applied on a company basis rather than a jurisdictional one. Data may be transferred to a company which is certified (strictly, which self-certifies) as a "safe harbor" or under a model contract clause or (between branches of a single organisation) under binding corporate rules.

All of these are used to some extent, with most processing companies (including OutIndex) self-certified as safe harbors and with model clauses and corporate rules governing the transfer. Anecdotally, a large quantity of data slips out in personal baggage, with – so far – no-one caught, publicly at least, in a compromising position.

The problem derives in part from the broadness of the EU rules, which makes it hard to give a definitive view as to whether any particular circumstance is covered by an exemption, by the personal nature of the penalties and the size of the fines (up to €300,000 in some countries, to say nothing of possible jail sentences), by the weakening of control implicit in onward transfer from a safe harbor, and generally by the lack of precedent and authority.

2.3 Cultural Difficulties

Concerns about punishment are not the only issue here. Mainland European countries do not have the tradition of common law countries (including the UK and the US) of handing over documents at all, let alone those covered by privacy laws. Conversely, the US has no concept of privacy in a workplace context (non-work data is a different matter). The time-limits and other expectations of US courts, however reasonable they may seem from the perspective of those courts, can easily come across as a form of commercial imperialism in the EU. Apparently trivial matters almost of etiquette (describing someone else's language as "foreign", for example) do nothing to endear US lawyers and regulatory authorities to those who are beyond their jurisdiction and unaffected by their imperatives, but who are very much subject to EU regulations.

3 Solutions

3.1 Readiness and Patience

The reality is that most of the concerns derived from EU privacy laws can be met. The issue is personal data not all data, and one obvious answer, albeit a long-term one, is for companies with European off-shoots to institute company-wide policies which allow them to identify data which is or may be personal data at the moment of creation or as a rolling matter by a mixture of technology and process. That is beyond the scope of this paper, and extends into considerations as to whether the data should be held at all, let alone transferred.

It is also possible to negotiate the terms on which data may be transferred, either by obtaining the express (and unforced) consent of the data subject and/or by agreement e.g. with German Works Councils.

The first of these often involves urging companies to bolt stable doors when the horse has gone. The second takes time. Neither is much help when the US court or regulator is demanding instant compliance with its orders.

3.2 Processing in the EU

If it is too late to apply a document retention policy, and too urgent to negotiate a compromise, the obvious answer to do the primary processing within the EU with a view not just to identifying the data which potentially offends the privacy laws but also to making the first-pass cull of data which is irrelevant anyway. That, properly done, will pull out the material which needs further consideration and allows the residue to be exported without risk of offence, or at least, with a much-diminished risk.

The expectations of a company offering such a service include a swift and defensible collections process, technology capable of identifying documents in specific classes or

categories, non-English language support, and knowledge of both the US requirements and the EU constraints. It also requires a feel for the cultural differences which confound so many of these operations. Lastly, of course, the service must be cost-effective.

3.3 The role of OutIndex in EU processing

There are, of course, a few companies, mainly large and US in origin, capable of meeting all or most of these requirements. The attractions of OutIndex are that it is primarily a software company able to tune its applications to the circumstances, that its origins are in the UK, and that its relatively small size and narrow niche fits it well to be a component in the overall process which leaves all the subsequent options e.g. as to the choice of review platform, open.

4 Conclusion

EU privacy concerns bulk large in the eyes of US lawyers and others who need to access and process large amounts of data of EU origin in a hurry. The subject rightly causes concern, even in an internal EU context, but there one can at least apply search and processing functions to identify potentially offending items. An additional layer of unlawfulness arises if the data is exported.

Processing the data within the UK with an eye in particular to privacy considerations is one way of mitigating the scope for an offence. A niche data processing company with feet on both sides of the Atlantic, as OutIndex has, is one obvious way to addressing the problem.

Chris Dale

The e-Disclosure Information Project
Oxford, England
8 October 2008