Dealing with data breaches in Europe and beyond

Ann Bevitt, Karin Retzer and Joanna Łopatowska
Morrison & Foerster LLP

REASONS FOR DATA PROTECTION LAW COMPLIANCE

The use of increasingly advanced technology means that the ways in which data breaches occur are becoming more difficult to prevent and track. Influenced by the US model, a growing number of European Economic Area (EEA) countries are developing rules on data breach notification. The member states of the EEA currently are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK. Croatia is set to join the European Union on 1 July 2013.

In Europe, “data breach” generally refers to instances where personal data has been subject to unauthorised access, collection, use or disclosure. Data breaches can be caused by inadvertent or deliberate actions that result in data being stolen, lost or disclosed, such as theft of storage devices, infiltration (hacking) of computer systems or inadequate data security practices. Notification of a data breach serves different purposes. The main purpose of notifying public authorities is to enable them to exercise their regulatory oversight functions, such as identifying security problems and taking actions to address them. Notifying individuals aims to enable them to mitigate the risk of harm caused by the breach. In addition, notification can serve to motivate organisations to implement more effective security measures to protect personal data.

Organisations operating in multiple jurisdictions face the difficulty of ensuring compliance with numerous different laws. This often requires implementing internal mechanisms to deal with breaches and to minimise costs. The costs of handling and mitigating the effects of a breach can be significant; and can include the costs involved in sending notices, dealing with regulatory investigations, employing external auditors, facing class action litigation and being involved in sending notices, dealing with regulatory investigations.

Against this backdrop, this chapter:

- Gives an overview of the EU/EEA legal framework concerning breach notification and local breach notification requirements.
- Considers global trends concerning the emergence of data breach legislation.
- Provides some guidance on preparing a data breach response plan.

CURRENT EU/EEA LEGAL FRAMEWORK

There is no general breach notification requirement in Directive 95/46/EC on data protection (Data Protection Directive). In the absence of explicit legislation, the need to introduce mandatory breach notification has been debated for several years by European regulators. In 2009, as part of the review of the EU telecommunications regulatory framework, Directive 2002/58/EC on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive) was amended to include mandatory data breach notification for electronic communications operators and internet service providers (ISPs) (see box, ISPs and telecommunications operators in the EU: mandatory breach notification).

In addition to these sector-specific rules, in the course of the review of the EU data protection framework, the European Commission (Commission) on 25 January 2012 published a proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation Proposal) (see http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf). The Regulation would replace the Data Protection Directive and there would be no need for harmonisation of minimum standards across the EU/EEA. EU Regulations are directly applicable and do not require transposition into local laws.

The General Data Protection Regulation Proposal introduces a broad breach notification requirement for any personal data breach similar to that set out in the amended ePrivacy Directive:

- **Trigger and Timing.** Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed must be notified to the local data protection authority without undue delay and no later than 24 hours after the controller becomes aware of the breach. A delay in notification is possible, but the controller must make a reasoned justification for taking longer than 24 hours to notify. Individuals must be notified without undue delay after the controller has notified the authorities, where the breach is likely to adversely affect the protection of an individual’s personal data or privacy. Importantly, the Regulation explicitly mandates processors to notify controllers immediately about a breach on their side.

- **Content.** Notification must include the nature of the breach including the types of data and individuals concerned, possible consequences, contact details, measures taken to mitigate potential adverse effects and measures taken by the organisation.

- **Exemptions.** Notification to individuals is not required where the organisation can demonstrate that it applied appropriate protection measures to protect the data. As a result, an exemption from notification to individuals seems
to be available where encryption technology is applied.

- **Sanctions.** Failure to report a breach is sanctioned by administrative penalties of up to 2% of an organisation’s annual global turnover. For a first and unintentional breach (non-compliance with the Regulation), no sanction is imposed, only a written warning issued, where, for example, a company with fewer than 250 employees is processing data only as an activity ancillary to its main activities.

Before the proposed Regulation becomes EU law, both the European Parliament and the Council of the European Union must jointly agree on the final text in the co-legislation procedure. Therefore, changes to the proposal are likely. In addition, under the current draft, the Commission will lay down other detailed requirements specifying the circumstances for mandatory breach notification and a standard notification format. There is a common expectation that the final law will be adopted before the Parliament’s term ends in summer 2014, and is likely to become operational two years after the adoption date.

**LOCAL BREACH NOTIFICATION SCHEMES**

While there is currently no general breach notification requirement across the EU/EEA, specific member states have taken a number of different approaches to the issue. Some countries have adopted statutory laws that oblige organisations to report data breaches. In other countries only voluntary guidance issued by the data protection authorities exists. Other member states are still considering whether and how to introduce breach notification obligations.

The overview below outlines selected approaches that have been taken (whether mandatory or voluntary) across the EU/EEA.

**Mandatory breach notification**

The following jurisdictions oblige organisations to report data breaches:

- **Austria.** Since January 2010, it has been mandatory for private and public sector organisations in Austria to notify individuals “without undue delay” and “in adequate form” if and when the organisation becomes aware of a “systematic and serious misuse of data” that may “cause damage to the data subject” (section 24(2a), Federal Data Protection Act (Datenschutzgesetz 2000)). Notifying data protection authorities is not mandatory. Notification is not required where the harm is minor, the breach is incidental, or the cost of informing the individuals would be disproportionate.

- **Germany.** Data breach notification was introduced in Germany in 2009 (section 42a, Federal Data Protection Act (Bundesdatenschutzgesetz) (BDSG)). The law applies to private sector businesses and certain federal state agencies (for example, public electricity providers). Both individuals and data protection authorities must be notified immediately (that is, without undue delay). Notification is required for breaches that may lead to “serious impediments for privacy and other individual interests”. The requirement applies to personal data. The types of data, as well as the possible consequences of the breach (for example, damages or identity theft) must be taken into account when determining whether such “serious impediments” exist. The notification obligation is triggered when the breach involves:
  - sensitive data;
  - criminal records;
  - bank account or credit card data;

- **Spain.** Different from other countries, Spanish law (Royal Decree 1720/2007) sets out a mandatory procedure for management of data breaches but does not require notification of the data protection authority or the individuals. Data controllers and processors in all sectors must establish an internal registry to record:
  - the type of incident and the time it occurred or was detected;
  - the effects of the breach;
  - the corrective measures applied; and
  - a record of the individuals notified (if the organisation chooses to notify individuals).

**Voluntary breach notification**

The following jurisdictions allow for voluntary reporting of data breaches:

- **Denmark.** The Danish procedure for reporting data breaches is based on several decisions issued by the data protection authority. If the breach involves sensitive data, data about criminal offences, serious social problems, or purely private matters, notification is most likely necessary, unless the affected individuals are already aware of the breach. Breaches of non-sensitive data are not always reported in practice. When determining whether to notify, organisations should take into consideration the possible effects and extent of the breach. Organisations should notify all affected individuals as soon as reasonably possible, and where the personal data has become available in publicly accessible sources, ensure that it is removed from such sources.

- **Ireland.** Under the Data Protection Commissioner’s (Commissioner) voluntary Breach Notification Guidance (Guidance) and Personal Data Security Breach Code of Practice (Code), the Commissioner should be notified about breaches involving any personal data. The best practices suggested by the Guidance and the Code apply to all private organisations. It is recommended that the Commissioner is notified as soon as the organisation becomes aware of unauthorised or accidental disclosures of customer or employee personal information, although an exception is made when:
  - the data subjects have already been informed;
the loss affects no more than 100 data subjects; or
- the loss involves only non-sensitive, non-financial personal data.

At the outset, the Commissioner does not require a full report, only an email providing a general description of the incident. This notification is expected within two working days and may be followed by a full report on request. The Commissioner decides whether and how the affected individuals should be notified (if the organisation has not already done so). Where the Commissioner is not notified, the organisation should maintain (centrally) a brief summary of each data security breach incident, including an explanation of the basis for not informing the Commissioner.

- **Italy.** In May 2011 Italy's data protection authority, the Garante, published guidance (Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie) addressed to the banking sector advising banks to promptly notify the Garante about any significant illicit event in data management given the number of affected individuals, or amount and types of compromised data. Individuals should be notified without delay if notification is necessary to defend their rights. As opposed to mandatory, the notification duty is described as “opportune”. Therefore, it is unclear whether and what type of sanctions would result from a failure to notify.

- **UK.** The UK Information Commissioner's Office (ICO) issued non-binding guidance on how organisations should manage and notify a data security breach (Guidance on data security breach management, updated in July 2011, and Guidance on Notification of Data Security Breaches to the ICO, updated in July 2010). The ICO recommends that all “serious” breaches are brought to its attention. A “serious” breach is determined based on the potential for harm to individuals, the number of individuals affected by the breach, and the sensitivity of the data. While the guidance does not specify the types of personal data that would trigger notification, it notes that there is likely to be a significant risk of substantial harm when sensitive data or financial information is involved. The guidance does not specify a timeframe for notifying the ICO and/or the affected individuals, or the method of notification. Although the breach notification guidance is voluntary, it should be diligently observed to minimise the risk of penalties.

Since April 2010, the ICO has had the power to impose monetary penalties of up to GB£500,000 for breaches of the Data Protection Principles enshrined in the UK Data Protection Act (as at 1 March 2012, US$1 was about GB£0.8). Penalties that have been levied include:
- for faxing highly sensitive personal information to the wrong recipients: GB£100,000;
- for the loss of an unencrypted laptop containing personal information relating to 24,000 individuals: GB£60,000;
- for emailing sensitive personal information to incorrect recipients on three occasions: GB£120,000;
- for emailing highly sensitive personal information about a large number of vulnerable people to 23 unintended recipients: GB£80,000.

Almost all of the organisations that have been fined to date are local government entities.

**GLOBAL TRENDS**

For organisations that operate in multiple jurisdictions, handling data breaches becomes particularly challenging if the affected individuals reside in a number of different jurisdictions, or if various laws or practices apply to the reporting of data breaches.

Current EU rules on applicable law provide no easy solutions to this challenge. Under the Data Protection Directive, the principal criterion for determining applicable law is the place of establishment of the organisation controlling the processing, largely irrespective of where the data processing occurs. In addition, if the controlling organisation is not established in the EU/EEA but makes use of equipment located there to process data, the relevant member state’s law applies. In its opinion on applicable law (Opinion No 8/2010 on applicable law, 16 December 2010), the Article 29 Working Party expanded on this and argued that where data are collected by multiple affiliates of a non-EU/EEA organisation in a number of EU/EEA member states, those affiliates must comply with the rules applicable in each member state where data collection takes place.

Under the General Data Protection Regulation Proposal, the EU/EEA rules would apply not only to controllers and processors established in the EU/EEA but also to controllers established outside the EU/EEA but whose processing targets EU/EEA residents or monitors their behaviour (usually in an online context). Making use of equipment in the EU/EEA would no longer be relevant for determining applicable law.

At present, mandatory breach notification obligations outside the EU/EEA exist in Mexico, the US and the United Arab Emirates (Dubai International Financial Centre). In Canada, New Zealand and Australia breach notification is voluntary, but this may soon change. In Japan two approaches exist. The core elements of breach notification obligations in these jurisdictions are set out below (see Voluntary breach notification: Japan – mixed model).

**Mandatory breach notification**

The following jurisdictions oblige organisations to report data breaches:

- **Mexico.** As of 1 January 2012 a new comprehensive Law on the Protection of Personal Data is in force in Mexico (Federal Law on Protection of Personal Data Held by Private Parties, Official Gazette of 5 July 2010). The law requires organisations to immediately notify individuals about security breaches that “materially affect [their] property or moral rights”. According to the implementing regulations (Regulations implementing Federal Law on Protection of Personal Data of 21 December 2011), the notification requirement is triggered by any loss, theft or unauthorised use, modification, access, copying, destruction, damage, or alteration to personal data. Neither the law nor the implementing regulations are clear as to whether the data protection authority must also be notified.

- **United Arab Emirates.** Limited breach notification obligations were introduced in 2006 (Dubai International Financial Centre Law No 1 of 2007) and apply only within the Dubai International Financial Centre. Under this law, organisations must notify the Commissioner of Data Protection as soon as reasonably practicable about any unauthorised intrusion into any database containing personal information. Any data breach requires notification to the authorities, but there is no obligation to notify the affected individuals.
**United States.** In the United States, 46 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands have enacted laws imposing notification obligations on organisations that discover, or are themselves notified about, a breach of security involving personal information. Many of these state laws are modelled on the California security breach notification law (California Law), which came into force on 1 July 2003 (Cal. Civ. Code § 1798.82). The California Law made it mandatory to provide notification of security breaches involving unauthorised acquisition of computerised data that included certain types of personal information relating to individuals residing in California. The affected individuals must be notified as soon as possible, but the law does not apply to any public authorities. The California Law was recently amended to require notice to the California Attorney General where more than 500 California residents must be notified as a result of a single security breach.

Most other US state security breach laws require organisations to notify individuals of a security breach in which certain types of personal information were, or are reasonably believed to have been, acquired by an unauthorised person. Nonetheless, a number of states do not require notification when the security breach is not likely to cause harm, such as identity theft.

In addition to California, 14 states require notification to a state authority, such as the state Attorney General. Unlike the California Law, however, most of these 14 states do not set a threshold of state residents that must be met in order to trigger the obligation to provide notice to the state authority; notifying the relevant authority is mandatory regardless of the number of individual state residents affected.

**Voluntary breach notification**

The following jurisdictions allow for voluntary reporting of data breaches:

- **Australia.** Under the voluntary guidance issued by the Office of the Privacy Commissioner of Australia in August 2008 (Guide to handling personal information security breaches), organisations are encouraged to report significant breaches to the Office of the Australian Information Commissioner.

  Individuals should be notified if the breach creates a real risk of serious harm. There is no clarity on what this implies. The guidance only advises that some information such as that concerning health or financial accounts may be more likely to cause individual harm. The introduction of mandatory breach notification is being discussed; however, the government has not yet published any proposal.

- **Canada.** Under the voluntary guidelines issued by the Federal Privacy Commissioner in August 2007 (Key Steps for Organizations in Responding to Privacy Breaches), individuals should be notified as soon as reasonably possible where a breach presents a risk of harm. Informing the Privacy Commissioner is only encouraged.

  The draft bill of May 2010 amending the Personal Information Protection and Electronic Documents Act, if adopted, would require organisations to report to the Federal Privacy Commissioner, “any material breach of security safeguards involving personal information under its control”. Organisations would need to consider the sensitivity of the information, the number of individuals involved and the cause of the breach. Individuals would need to be notified if it is reasonable to believe that the breach creates a real risk of significant harm, broadly defined to include financial and psychological effects.

- **New Zealand.** In February 2008 the New Zealand Privacy Commissioner issued voluntary breach notification guidelines that apply to private sector organisations. In the event of a breach individuals should be notified as soon as reasonably possible when there is a foreseeable risk of harm (Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist). Notifying the Privacy Commissioner is recommended. The guidelines recommend considering the sensitivity and context of the information involved in the breach and how the information could be used (for example, for fraudulent or harmful purposes).

- **Japan – mixed model.** In Japan, two models exist, depending on the authority to which the breach must be notified. Under the Financial Services Agency's (FSA) guidelines revised in 2009, applicable to financial services providers only, breach notification is mandatory. Government authorities must be immediately notified about all data breaches, regardless of their size or severity. Individuals must be notified promptly, and a public announcement must follow. The guidelines do not provide exceptions for encrypted data.

  Although there is no explicit requirement for breach notification under Japan’s Act on the Protection of Personal Information, the Ministry of Economy, Trade and Industry’s (METI) revised guidelines (2008) recommend notification with reference to the Act’s security requirements. Private sector businesses are recommended to provide notice, but notification is not expected when the rights and interests of the individuals have not been or are not likely to be infringed by the breach, for example, when data was recovered immediately or when advanced encryption was used.

**PREPARING A DATA BREACH RESPONSE PLAN**

The variety of legal regimes and the risk of negative consequences caused by data breaches should encourage organisations to prepare an incident response plan for dealing with breaches. When a breach occurs, a response plan serves as a reference guide for best practices in dealing with the breach, as well as on how to identify and comply with the relevant legal requirements. Set out below is a model procedure that organisations can use to create their own response plans.

**Preventing a breach**

Organisations should take reasonable measures to prevent data breaches. It may be helpful to draw up a response plan of best practices that at a minimum should comprise the following steps:

- **Define the breach.** Identify the areas where the breach is likely to occur (for example, physical or IT security) taking into account the nature of the processing. “Data breach” can be defined as any situation in which the confidentiality of internal information:

  - may have been compromised (for example, disclosed to, accepted by or acquired by an individual who is not authorised to access or receive the information); or

  - is at risk of being compromised.

  It is also important to identify the data types and the individuals whose data may be compromised.

- **Secure the system in advance.** Train and supervise employees to ensure security controls, and ensure that all
appropriate security measures are in place. Among others, risks to consider when evaluating and implementing security measures may include:

- access to sensitive files by employees and independent contractors;
- use of security controls by employees;
- transmission, storage and disposal of computerised data;
- outsourcing transactions that require transmission of data;
- insufficient physical security of the premises; or
- risk of unauthorised access.

- Ensure appropriate agreements with service providers. Ensure that agreements with service providers (data processors) include appropriate security measures and a duty to notify your organisation about any breach that occurs on their side.

- Create a response team. Establish a response team composed of the relevant IT and physical security personnel, legal counsel and human resources personnel. Assign responsibilities to each member of the team so that when a breach occurs they know how to proceed. It may be helpful to draft rules of procedure describing their duties and procedures that must be followed.

- Ensure efficient communication. Inform employees about when, how and to whom they must report a data breach.

Response measures: dealing with a data breach

Whatever the type of data breach, be it the loss of a laptop or data stolen from an organisation's premises, certain best practices should be followed to mitigate the effects. Once a breach has been identified, a number of different issues should be addressed, the most critical of which is ensuring compliance with the applicable laws. However, even where no such laws exist, following a procedure may help to resolve the breach efficiently, and at minimum cost. The following steps constitute a model procedure for data breach response:

- Gather necessary information. Gather as much information as possible to assess the breach. This should include:
  - affected data types;
  - affected information systems and sensitivity of data contained therein;
  - number and identity of affected individuals and their contact details; and
  - possible consequences of the breach.

- Take initial steps. Determine whether the breach is ongoing and implement measures to retrieve exposed data, block access to and secure data to prevent any additional exposure. Launch an internal investigation, and task the response team with their assigned duties. Prepare a report describing the breach and its scope.

- Verify applicable laws and guidance. Verify which laws imposing breach notification apply to the breach, and identify any applicable guidance from data protection authorities. If your organisation operates or has clients in multiple jurisdictions, ensure that all applicable laws have been taken into account. Under some laws, notification may not be required where data is encrypted or anonymised, if the breach affects only a small number of individuals or if the data types do not require particular protection. Determine whether such exemptions apply.

- Determine who to notify. Establish whether public authorities and/or the affected individuals must be notified, or whether any exemptions apply. Where individuals must be notified, establish how many individuals have been affected, what data types were involved and whether the breach will have a negative effect.

- Determine when to notify. Check the applicable law(s) to determine how quickly authorities should be notified. Most laws or guidance stipulate short notification deadlines, for example “as soon as possible” or “without undue delay”; in practice, this can mean anything between two days and a week.

- Determine format of notice. Check how data protection authorities and individuals must be notified. The format may vary depending on the context and applicable laws. Notifications to data protection authorities vary (for example, between a full report and a short email). Personalised emails or telephone calls may be necessary to notify individuals, but where a significant number of individuals are affected, a communication in the press may be sufficient.

- Determine content of notice. Ensure that any notice addressed to individuals contains:
  - a description of the breach and types of data concerned;
  - measures taken to respond to the risks; and
  - recommendations on how the individual can further mitigate any adverse effects.

- Ensure that any notice addressed to authorities describes:
  - the consequences of the breach;
  - measures proposed or taken to resolve the breach; and
  - security measures in place at the time of the breach.

- Optimise notifications and communication. Consider a service provider to deal with notifications to individuals. This might include:
  - mail merges;
  - printing, sorting and mailing; and
  - secondary notification where addresses have changed and letters or emails bounce.

Consider engaging a public relations company that could analyse any media coverage, manage subsequent responses and minimise any potential damage to your organisation's reputation.

The breach report

Some laws require records to be maintained after all necessary steps to resolve the breach and its consequences have been completed. These records should usually describe the breach, the response and the remedial measures taken to prevent recurrence. Even if there are no such requirements, it is good practice to document the handling of the breach. Internal evaluation of this documentation may be helpful to avoid future similar occurrences, and to modify the response plan accordingly.
ISPS AND TELECOMMUNICATIONS OPERATORS IN THE EU: MANDATORY BREACH NOTIFICATION

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive) (ePrivacy Directive), amended in 2009 by Directive 2009/136/EC on consumer protection and users' rights in relation to the processing of personal data and the protection of privacy in electronic communications (Citizens' Rights Directive) introduces mandatory breach notification to data protection authorities and individuals, but only for “providers of publicly available electronic communications services”. While the ePrivacy Directive is aimed at telecommunications operators and ISPs, its broad wording, in particular the definition of electronic communications services, could be used by national regulators to bring other services under its regimen. For example, internet cafés or hotels allowing guests to use communications devices, universities facilitating use of the internet, or employers providing internet access to their employees.

### Notification obligations under the ePrivacy Directive

The amended ePrivacy Directive broadly defines “data breach” to include any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. The following rules apply:

- **Trigger.** The local authority must be notified every time a breach occurs, that is, there are no thresholds and no limitations as to data types covered. The affected individuals should be notified only when the breach is “likely to adversely affect their personal data or privacy”. This formulation is ambiguous, in particular on how the seriousness of a breach should determine the level of response.

- **Timing.** Both the national authorities and the affected individuals should be notified without undue delay. This is not further specified in the ePrivacy Directive but it is likely that most member states will impose short deadlines.

- **Content.** The notification should describe the nature of the breach, its consequences and the measures proposed or taken to address it, as well as contact details of the organisation. Notice to individuals must also include recommendations on how to mitigate possible adverse effects. In addition, providers must keep records of data breaches documenting the relevant facts, the effects of the breach and the remedial actions taken.

- **Exemptions.** Providers are exempt from the obligation to notify only when they are able to prove “to the satisfaction of the competent authority” that appropriate technological protection measures to secure the data were in place. These measures must render the data unintelligible to any person who is not authorised to access the data, for example, through encryption.


### Implementation of the Directive

Member states had until 25 May 2011 to transpose the amended ePrivacy Directive into national law. However, many states have not yet managed to do so. Notably, implementing laws exist in Austria, the Czech Republic, Denmark, Estonia, Finland, France, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Slovakia, Spain, Sweden and the UK.

The member states that have implemented the ePrivacy Directive have not chosen to broaden the scope to impose mandatory breach notification on other sectors. Most of the implementing laws mirror the wording of the Directive.

In their implementing legislation, many member states authorise relevant national authorities to issue guidance on the circumstances, format and procedures applicable to the notification requirements. Some member states envisage a broader scope for the guidance than that provided for by the Directive. For example, the Estonian data protection authority has the power to introduce exceptions to the notification obligation.
ANN BEVITT
Morrison & Foerster LLP
T +44 20 7920 4041
F +44 20 7496 8500
E abevitt@mofo.com
W www.mofo.com

Qualified. England and Wales, 2000
Areas of practice. Privacy and data security; employment.
Recent transactions
- Advised a multinational manufacturer of pharmaceutical, diagnostic, therapeutic, surgical and biotechnology products on the employment and privacy aspects of its HR outsourcing, including the review of HR policies in more than 80 countries worldwide.
- Advised an international recruitment corporation on data protection issues arising out of the collection of applicant data and diversity monitoring.
- Advised HMRC on the employment and human resources issues arising out of one of Europe’s most high-profile technology outsourcing and re-procurement projects.

KARIN RETZER
Morrison & Foerster LLP
T +32 2 340 7364
E kretzer@mofo.com
W www.mofo.com

Qualified. Munich bar, Germany, 1997; EU list of the Brussels bar, 2000
Areas of practice. Privacy and data security; advertising and marketing law.
Recent transactions
- Assisted client with centralising its global HR data, including all global data protection and information security considerations in over 80 countries.
- Advised client on appropriate responses to data breaches in multiple jurisdictions.
- Counselled on data protection strategies, including binding corporate rules and contracts with affiliates and vendors.
- Advised client on direct marketing initiatives including viral marketing and social media.
- Advised on requirements for behavioural advertising techniques and analytics tools on the use of specific content.

JOANNA ŁOPATOWSKA
Morrison & Foerster LLP
T +32 2 340 7365
E jlopatowska@mofo.com
W www.mofo.com

Qualified. Wrocław bar, Poland, 2005; EU list of the Brussels bar, 2010
Areas of practice. Privacy and data security; advertising and marketing law.
Recent transactions
- Advised client regarding obligations under privacy laws including registrations with local data protection authorities, privacy policies and procedures, data breaches and cross-border data transfers.
- Advised client in rapidly evolving areas of privacy regulation such as social media, user generated content and online behavioural advertising techniques and analytics tools.
- Advised client on the collection, use and disclosure of employee information, including the centralisation of HR data in global organisations.