PRACTICAL LAW COMPANY®

Dealing with data breaches in Europe and beyond

www.practicallaw.com/6-505-9638

Karin Retzer and Joanna Łopatowska
Morrison & Foerster LLP

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 EU and European Economic Area (EEA) countries are developing rules on data breach notification. In Europe, "data breach" generally refers to instances where personal data has been subject to unauthorised access, collection, use or disclosure. Data breaches may 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 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 at enabling 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.

In Europe, approaches to data breach notification vary. There are countries with statutory law and guidance on breach notification requirements across sectors. In other countries, neither specific rules nor guidance exist.

In the EU, member states are in the process of implementing the amendments to Directive 2002/58/EC on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive), which introduce a breach notification requirement for providers of publicly available communication services, such as internet service providers and telecommunication operators. Mandatory breach notification may soon be introduced for other sectors at the EU/EEA level.

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; these can include the costs involved in sending notices, dealing with regulatory investigations, employing external auditors, facing class action litigation and losses experienced as a result of decreased customer confidence.

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.

EU/EEA LEGAL FRAMEWORK

There is currently 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 (a package of legal instruments comprising six directives and one regulation), the Privacy and Electronic Communications Directive was amended to include mandatory data breach notification for electronic communications operators and internet service providers (*see box, ISPs and telecommunications operators in the EU: mandatory breach notification*). Member states have until 25 May 2011 to transpose the amendments into national law. Importantly, Recital 59 of the amended Privacy and Electronic Communications Directive expressly calls for this obligation to be extended to other sectors.

Following up on this call to extend the obligation, the European Commission (Commission), in its ongoing review of the European data protection framework, published a Communication outlining, among other things, its intention to introduce a general data breach notification obligation (A comprehensive approach on personal data protection in the European Union COM(2010) 609 final, 4 November 2010). Unfortunately, the Commission did not specify the scope of this obligation, in particular who should be notified and the criteria that would trigger the notification obligation.

All EU institutions and advisory bodies generally support mandatory breach notification applying to all sectors. The Commission is expected to present its proposal to the European Parliament and the Council of the EU in 2011, both of which must agree on the final text in the co-legislation procedure (*Article 16, Treaty on the Functioning of the European Union [2008] OJ C 115/47*). Once the legislation is published, it will be months before it is adopted and implemented in the member states (if a directive is proposed, its implementation may take several years for all countries to implement.

LOCAL BREACH NOTIFICATION SCHEMES

There is no general breach notification requirement across the EU/EEA, and 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. Yet other member states are still considering whether and how to introduce breach notification obligations.

The overview below outlines the approaches that have been taken (whether mandatory or voluntary) across the EU/EEA, focusing on:

- Notification triggers.
- The timing and content of notification.
- Who must be notified.
- Whether any exemptions apply.

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)*). The limitation to "systematic and serious misuse" suggests that when the breach is incidental, notification is not necessary. Notification is only required when the organisation knows about the breach, for example, when a member of the management board has actual knowledge. In addition, notification is not required in the case of any of the following:
  - the data breach only results in non-economic damage;
  - potential damage is minor;
  - the cost of informing all individuals would be disproportionate.

  Notifying data protection authorities is not mandatory.
- **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;
  - personal data that is subject to legal privilege (for example, data held by lawyers, doctors or journalists); or
  - data collected on users of online services.

  In cases where a large number of individuals are affected, public announcements in at least two national newspapers may replace individual notices.
- **Norway.** Norway was the first country in the EU/EEA to introduce mandatory breach notification for public and private organisations (*sections 2 to 6, Data Protection Regulations on the processing of personal data, 4 November 2005*). The obligation only covers data requiring confidential treatment, including sensitive data such as:
  - medical and health data;
  - information on race or ethnic origin;
  - political or religious beliefs;
  - union membership.

  The notification requirement is triggered by any "discrepancy", which includes a breach resulting in unauthorised disclosure of personal data where confidentiality is necessary. The data protection authority must always be notified. However, there is no obligation to notify individuals, unless the data protection authority instructs the organisation to do so. This is decided based on the nature and quantity of personal data disclosed. The law does not provide any specific deadline for notification, but the authority expects notification within a week of the incident. Causes of the breach and measures taken to mitigate it must be documented.
- **Spain.** In 2007, mandatory security measures for data controllers and processors were introduced for both the public and private sectors (*Royal Decree 1720/2007*). The law set out a procedure for management of data breaches, including:
  - establishing 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).

  However, in practice, the level of information that must be recorded depends on the nature of the personal data concerned. There is no obligation to notify the data protection authority or the affected 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 given by the data protection authority. In principle, all types of personal data are covered, but the voluntary nature of the guidance means that in practice not all breaches are reported. However, 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. In addition to the type of data, organisations should take into consideration the possible effects of the breach, and the extent of the breach when determining whether to notify. Organisations should notify all affected individuals as soon as reasonably possible, either directly or indirectly.

Organisations should also examine whether the information has become publicly available and, if so, ensure that the information is removed from publicly accessible 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; and
  - the loss involves only non-sensitive, non-financial personal data.

  At the outset, the Commissioner does not require a full report, only an e-mail 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. After notification, the Commissioner decides whether the affected individuals should be notified (if the organisation has not already done so), and how this notice should be provided. Even in circumstances 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.
- **UK.** In March 2008, the UK Information Commissioner's Office (ICO) issued non-binding guidance on how organisations should manage a data security breach and when to notify the ICO of these breaches. 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 are 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 (as at 1 April 2011, US$1 was about GB£0.6) for breaches of its Data Protection Principles, which are enshrined in the UK Data Protection Act. The first penalty, of GB£100,000, was levied in a case where local council employees faxed highly sensitive personal information to the wrong recipients. The ICO issued its second penalty (GB£60,000) to an employment services company for the loss of an unencrypted laptop that contained personal information relating to 24,000 people who had used community legal advice centres. Two further penalties, of up to GB£80,000 each, have been levied on two more local authorities, where one local authority provided a service for the other, and where two unencrypted laptops containing the details of around 1,700 individuals were stolen from an employee's home.

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 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 its opinion on applicable law (*Opinion No 8/2010 on applicable law, 16 December 2010*), the Working Party 29 expanded on this and argued that where data are collected by multiple entities in a number of EU/EEA member states, those entities must comply with the rules applicable in each member state where data collection takes place. The Commission is likely to address this issue in the new rules resulting from its review of the data protection framework.

Until that happens, it seems that the data controller responsible for the breach needs to comply with each set of requirements in each of the countries where a breach affects individuals. In addition, if the controller is not established in the EU/EEA but makes use of the equipment located there to process data, the relevant member state law applies.

Rules on applicable laws for breach notification obligations outside the EU/EEA are generally based on the location of the affected individuals.

At present, mandatory breach notification obligations outside the EU/EEA exist in the US, United Arab Emirates (UAE) and Japan. In Canada, breach notification is voluntary, but mandatory notification is currently being discussed by the parliament. In other countries such as New Zealand and Australia, breach notification is voluntary, but legislation is being discussed. The core elements of breach notification obligations in these jurisdictions are set out below.

Australia

In Australia, the introduction of mandatory breach notification is being discussed. The Australian Law Reform Commission has proposed, among other things, that the Privacy Act be amended is include a breach notification obligation. However, the government has not yet proposed the relevant amendments.

In place of any legislation, voluntary guidance issued by the Office of the Privacy Commissioner of Australia in August 2008 applies (Guide to handling personal information security breaches). The guidance states that individuals should be notified if the breach creates a real risk of serious harm.

Organisations are encouraged to report significant breaches to the relevant authority (the Office of the Australian Information Commissioner (OAIC), which absorbed the Office of the Privacy Commissioner on 1 November 2010). There is no clarity on what specific data elements are covered. The guidance only advises that some information such as that concerning health or financial accounts may be more likely to cause individual harm. In other aspects, the Australian guidelines largely resemble those of New Zealand (*see below, New Zealand*).

Canada

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

Until the bill is passed, the voluntary breach notification guidelines issued by the Federal Privacy Commissioner in August 2007 apply (Key Steps for Organizations in Responding to Privacy Breaches). According to the guidelines, individuals should be notified as soon as reasonably possible where a breach presents a risk of harm. Informing the appropriate privacy commissioner is only encouraged.

Japan

In Japan, two models exist, depending on the authority to which the breach must be notified. Under the revised Financial Services Agency's guidelines, applicable to financial services providers only, breach notification is mandatory (the Financial Services Agency Guidelines became effective in 2005 and were later revised in 2009). 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.

In contrast, under the Ministry of Economy, Trade and Industry's guidelines notification is not mandatory, only recommended (revised guidelines have been effective as of February 2008). 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.

New Zealand

Voluntary breach notification guidelines issued by the New Zealand Privacy Commissioner in February 2008 apply to private sector organisations and recommend that 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).

UAE

In 2006, the Dubai International Financial Centre (DIFC) Authority amended its privacy law to include, among other things, limited breach notification obligations (Dubai International Financial Centre Law No 1 of 2007). The law applies only within the DIFC. 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.

US

In the US, more than 45 states have enacted laws imposing notification obligations on organisations that discover, or are themselves notified about, a breach of security of their information systems. In general, state security breach notification laws are understood to be modelled on the California Security Breach Notification Act (California Act), which came into force in July 2007 (Cal. Civ. Code § 1798.82 (LEXIS through 2007, ch. 12, June 7, 2007)). This law made it compulsory to provide notification of security breaches to consumers affected by the breach and residing in California. The affected individuals must be notified as soon as possible, but the law does not require notification to any administrative authority.

Most other US states require organisations to notify individuals of a breach in which certain personal information was or is reasonably believed to have been acquired by an unauthorised person. Several state laws, however, also impose notification obligations in case of a risk of harm to an individual, such as identity theft. Only a few states require notification to the authorities.

PREPARING A DATA BREACH RESPONSE PLAN

The variety of legal regimes and the risk of negative consequences caused by data breaches should encourage companies to prepare an incident response plan for managing these incidents. 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 companies can use to create their own response plans.

Preventing the breach

Companies should take reasonable measures to prevent data breaches, and draw up a plan of best practices to follow in the event of a breach. At a minimum, a data breach response plan should comprise the following steps:

- **Define the incident.** "Data breach" means 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.

  Depending on the nature of the organisation, the breach is usually related to physical or IT security.

  In addition to defining the breach, it is important to identify the data categories 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. 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;

Country Q&A

- outsourcing transactions that require transmission of data;
- insufficient physical security of the premises; or
- risk of unauthorised access.

- **Ensure appropriate contracts with service providers.** Ensure that agreements and contracts with third party service providers (data processors) include appropriate security measures.
- **Create a response team.** Establish a response team composed of the relevant IT security personnel, physical security personnel, legal counsel and human resources personnel. Assign a concrete role 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 responsibilities, as well as any specific procedures that must be followed.
- **Ensure efficient communication.** Inform employees about when, how and to whom they must report a data breach. Ensure that third party service providers are properly informed about the incident plan and procedures, and in particular of their responsibility to notify your organisation about any breach that occurs on their side.

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 an incident has been identified, a number of different issued 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:

- **Assess the incident and prepare a report.** Make an assessment of the data breach, its extent, the individuals it may affect and the possible consequences. Prepare a report describing the breach and its scope.
- **Take initial steps.** Block access to and/or secure personal data as soon as possible. Depending on the nature of the breach, this may involve either physical or IT security measures. Launch an internal investigation, and task the response team with their assigned duties.
- **Gather necessary information.** Gather as much information as possible. This should include:
  - types of data that were affected;
  - the affected information systems and sensitivity of data contained on those systems;
  - the number and identity of affected individuals and their contact details.

  In addition, determine whether the incident is ongoing and implement measures to retrieve exposed data or to prevent any additional data exposure.
- **Verify applicable laws and guidance.** Verify which laws imposing breach notifications apply to the incident, 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 were 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 provisions. Notifications to data protection authorities vary (for example, a full report, a short e-mail and so on). When notifying individuals, personalised e-mails or telephone calls may be necessary, 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 incident and type of data concerned;
  - the 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
  - the security measures in place at the time of breach.
- **Optimise notifications and communication.** Consider engaging an external service provider to deal with notifications to individuals. This could involve:
  - mail merges;
  - printing, sorting and mailing; and
  - secondary notification where addresses have changed and letters "bounce".
- **Consider engaging an external public relations company.** The company can analyse any media coverage, manage subsequent responses, and minimise any potential damage to your organisation's reputation.

The breach report

After all necessary steps to resolve the breach and its consequences have been completed some laws require records to be maintained. These records should usually describe the incident and the response, and the remedial measures taken to prevent recurrence. Even if there are no such requirements, it is good practice to document the management of the breach. Internal evaluation of this documentation may be helpful to avoid future similar occurrences, and the response plan could be modified accordingly.

ISPS AND TELECOMMUNICATIONS OPERATORS IN THE EU: MANDATORY BREACH NOTIFICATION

Directive 2002/58/EC on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive), which was amended in 2009 (by Directive 2009/136/EC) introduces mandatory breach notification to data protection authorities and individuals, but only for "providers of publicly available electronic communications services". "Electronic communications services" is defined as "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services". The Directive gives no further guidance on how to interpret the terms "publicly" or "normally provided for remuneration".

While the Privacy and Electronic Communications Directive is aimed at telecommunications operators and internet service providers, the broad wording could be used by national regulators to bring other services under its regimen. In particular, national interpretations are diverging for the purposes of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks (Data Retention Directive). As a result, some national regulators may bring organisations such as the following within the remit of the ePrivacy Directive:

- Internet cafes or hotels allowing guests to use communications devices.
- Universities facilitating the use of the internet.
- Employers providing internet access to their employees.
- Commercial website operators.

In contrast, some regulators are taking a narrower approach, which does not encompass the providers of free access to the internet such as hotels, housing societies, cafes or shops as is the case in Poland (based on information from the Ministry of Infrastructure of 28 February 2011 *(ŁT3m/0782-2/11)*).

Notification obligations under the Directive

The amended Privacy and Electronic Communications 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.** National authorities 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 in relation to 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 Privacy and Electronic Communications 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.

The Commission is expected to issue guidance on what the form and procedures of notification can take, after consulting with member states and the European Network and Information Security Agency (ENISA), an advisory body to the Commission. In preparation, ENISA published a report on data breach notifications in the EU (*www.enisa.europa.eu/media/press-releases/new-report-data-breach-notifications-in-europe*).

Implementation of the Directive

Member states have until 25 May 2011 to transpose the amended Privacy and Electronic Communications Directive into national law. However, although most of them have only draft texts (with the exception of Finland), none appears to have adopted legislation. It seems unlikely that the majority of member states will manage to implement the directive before the deadline.

In their draft texts, most member states have not broadened the scope of application to include mandatory breach notification for other sectors. Some member states have gone beyond the wording of the Privacy and Electronic Communications Directive, with the Czech Republic proposing to add "serious" as a threshold for breach notification, and Sweden proposing mandatory notification only if the breach "can be assumed to impact individuals to a larger extent". The German government, by contrast has proposed extending the obligation to notify "any breach of data protection", and not only limit notification to security issues or particular types of data (the bill is expected to be tabled in the Bundestag plenary at the end of May).

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).

CONTRIBUTOR DETAILS

KARIN RETZER

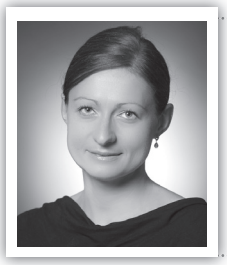
Morrison & Foerster LLP
T +32 2 340 7364
E *kretzer@mofo.com*
W *www.mofo.com*

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, 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 breach 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.