Whitepaper:

HOW EUROPEAN UNION DATA PROTECTION LEGISLATION AFFECTS YOUR DATA IN THE CLOUD

A primer for IT, security, compliance, and legal departments with a focus on the impact on cloud computing

"Enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy which can cut ICT costs, and when combined with new digital business practices, can boost productivity, growth and jobs."

European Commission Communication on cloud computing strategy, September 2011

This paper features content that was published in the May 2014 edition of StrategicRISK ‘Make IT Personal’, authored by Anthony Lee, a partner at DMH Stallard. The content is reprinted with permission.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>The Directive</td>
<td>4</td>
</tr>
<tr>
<td>Personal data</td>
<td>5</td>
</tr>
<tr>
<td>The New Regulation</td>
<td>6</td>
</tr>
<tr>
<td>Table comparing the current Directive with future Regulation</td>
<td>7</td>
</tr>
<tr>
<td>Overview on the right to share &amp; transferring data to third parties</td>
<td>7</td>
</tr>
<tr>
<td>Tokenized data</td>
<td>7</td>
</tr>
<tr>
<td>Security</td>
<td>8</td>
</tr>
<tr>
<td>Transferring data outside the EU</td>
<td>9</td>
</tr>
<tr>
<td>Safe jurisdiction (country) list</td>
<td>9</td>
</tr>
<tr>
<td>US Safe Harbor</td>
<td>10</td>
</tr>
<tr>
<td>Binding corporate rules (BCRs)</td>
<td>11</td>
</tr>
<tr>
<td>Self-assessment</td>
<td>11</td>
</tr>
<tr>
<td>Model contractual clauses</td>
<td>12</td>
</tr>
<tr>
<td>Individuals access to their own information (and the right of erasure)</td>
<td>13</td>
</tr>
<tr>
<td>Sanctions and private actions</td>
<td>14</td>
</tr>
<tr>
<td>European data protection seal</td>
<td>14</td>
</tr>
<tr>
<td>Transitional periods</td>
<td>15</td>
</tr>
<tr>
<td>Informing users and authorities of data loss</td>
<td>15</td>
</tr>
<tr>
<td>“Sensitive” personal data</td>
<td>15</td>
</tr>
<tr>
<td>Further information on the Regulation</td>
<td>15</td>
</tr>
<tr>
<td>Conflicting laws</td>
<td>17</td>
</tr>
<tr>
<td>Actions needed</td>
<td>18</td>
</tr>
<tr>
<td>First steps</td>
<td>21</td>
</tr>
<tr>
<td>Conclusion</td>
<td>21</td>
</tr>
<tr>
<td>Frequently asked questions</td>
<td>22</td>
</tr>
<tr>
<td>Finally – It’s never YOUR data</td>
<td>23</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Cloud computing has changed the workspace: it has provided increased value to enterprises by delivering business agility, greater co-operation between employees, and better consolidation of data across groups. The cost benefits of using cloud, its ease of use, and the fast deployment time of new services have seen every organisation using cloud services for important IT functions.

Cloud enables users to handle vast amounts of data, including personal data, on their customers, suppliers, and staff, to move the information around, and to share it domestically and internationally. With this comes increasing productivity for employees, but also increased threats to data; some threats are external (such as theft by hackers) and others are internal (such as accidental loss by employees).

In the European Union (EU), the main legislation on protecting data relating to people derive from the (EU Directive 95/46/EC). Whether an organisation is based in the EU, has branches in the EU, or provides services to EU residents, it needs to understand and conform to EU data protection laws. An organisation is responsible for ensuring that data is not compromised whether maliciously or inadvertently, by employees or by contractors, and if data is lost by a third party (e.g. by a cloud service provider), the organisation will be held responsible.

This white paper provides an introduction to the current Directive and to the recently proposed General Data Protection Regulation. It then outlines the steps required to ensure that both a firm’s data handling and specifically cloud usage and other types of data sharing are compliant.

This document is not a substitute for legal advice on data protection. It is strongly recommended to seek legal advice to ensure compliance.

---

2 European Parliament; P7_TA(2014)0212
INTRODUCTION

In 1995, the EU published the EU Data Protection Directive, which defines the framework for the processing of personal data on the 505 million EU residents across the 28 member countries.

By January 2012, a proposed draft General Data Protection Regulation was published. This is passing through the legislature process now, and it is expected that a final agreement on the document will be published in the summer of 2015 and implemented two years later. The new Regulation will harmonise the laws across the region and increase the maximum possible fines (possibly up to 5% of total global revenue or €1m, whichever is higher). Consequently, enterprises that conduct business with the EU or the European Economic Area (EEA), including cloud computing providers, need to be aware of the upcoming changes.

Skyhigh’s recently published European Q3 2014 Cloud Adoption and Risk Report\(^2\) indicates that approximately 75% of cloud service providers do not conform to the requirements of the Directive and therefore should not be used as repositories of personal data of EU residents.

THE DIRECTIVE

The Directive aims to protect people’s privacy and their personal data. Following its ratification, each EU country introduced national legislation to give it effect, albeit with some discretion as to its implementation. As a result, there are 28 different implementations, some of which are more light-touch than others.

Under the Directive, the data “controller” is responsible for any personal data it holds and for ensuring that the data is “processed” in accordance with the Directive’s requirements. A controller is the “person” that decides what to do with the data, such as a retailer that holds personal data on its customers. “Processing” is defined widely and includes collecting, holding, disclosing and using the data. “Personal data” is data by which an individual can be identified, such as a name and address.

The Directive also recognises the concept of the data “processor,” which processes data on behalf of a controller. A cloud service provider that stores data on behalf of a controller is an example of a processor. No obligations are currently imposed on the processor and, in most countries; the processor has no statutory responsibilities.

Data Controllers need to register with their appropriate government body. (In the UK, this is the Information Commissioner’s Office⁴).

**PERSONAL DATA**

As indicated above, “personal data” (commonly known as personally identifiable data or personally identifiable information [PID or PII]) is data by which an individual can be identified. As the Directive does not define personal data prescriptively, this has led to different interpretations in different countries. For example, some countries initially stated that work email addresses were not personal data. However, others have insisted that work email addresses can constitute personal data because they typically include the name of the person and the name of their organisation, which usually means that he or she can be identified. It is recommended that, to ensure an organisation complies with current (and new) data protection legislation, it must consider all information that names an individual, his/her address, and any contact details as personal data.

The data controller (person or organisation that “controls” the data) is responsible for the management of that data.

The Directive requires the controller to comply with a number of core principles. Arguably, the most important principle, which is a focus area of this paper, is that the data must be kept secure. Underpinning all of this is the principle that the personal data should be used only for the purpose for which it was originally collected.

⁴ [www.ico.org.uk](http://www.ico.org.uk)
THE NEW REGULATION

As indicated above, a new Regulation is currently making its way through the EU legislative process. On 3rd October 2014, the Ministers in the Justice and Home Affairs Committee of the EU’s Council of Ministers backed the plans as part of a wider partial agreement. Once it becomes law, it will take direct effect that means that it will automatically come into law two years later in the member states without the need for local implementation.

If adopted in its current form, the Regulation will be more prescriptive, place a heavier compliance burden on controllers and will impose statutory obligations on processors (such as cloud service providers) as well as on controllers. In other words, businesses falling short under the current rules will fall short under the new regime and face tougher sanctions.

Though there will no doubt be continual lobbying with regard to the Regulation (more than 200 amendments having been suggested so far), and the current draft may therefore change, the table below shows the areas of the Directive and expectations in the Regulation. This could have a major impact on data held in the cloud, cloud-based services and cloud service providers.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Directive</th>
<th>Expectations in the Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview on the right to share &amp; transferring data to third parties</td>
<td>In order for a controller to share data, one of several “fair processing” conditions must be satisfied. Enterprises (as controllers) looking to share personal data with cloud service providers (the data processors) e.g. for data storage purposes must satisfy one of these conditions. In the business world, the condition most relevant to data sharing is that it is necessary for the controller’s “legitimate interests”</td>
<td>A controller may still have data processed where the “legitimate interest” condition is satisfied. However, this is capable of being overridden in circumstances where the processing does not meet an individual’s (i.e. the person who is the subject of the data) reasonable expectations. There are also greater transparency obligations on the controller. For example, an enterprise using the services of a cloud service provider must: • <strong>Inform</strong> the individuals of their purported legitimate interests; • <strong>Remind</strong> individuals of their right to object to the sharing; and • <strong>Document</strong> their legitimate interests and any reminders made.</td>
</tr>
<tr>
<td>Tokenized data</td>
<td>No reference in the Directive</td>
<td>If data has been ‘tokenized’ or ‘pseudonymized’ to remove individual identifiers, processing is presumed to meet the individual’s reasonable expectations of privacy.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Directive</td>
<td>Expectations in the Regulation</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------------</td>
</tr>
</tbody>
</table>
| Security    | The controller must have 'appropriate organisational and technical measures' in place to protect any personal data in its charge against unauthorised processing, loss or damage. This includes:  
- Guarding against external threats (such as hacking);  
- Preventing internal threats (such as employees and consultants);  
- Patching vulnerabilities in IT systems (technical); and  
- Having appropriate policies and procedures in place (organisational).  
In relation to data sharing, whether domestically or internationally, the controller must satisfy itself that the recipient will keep the data secure (from both technical and organisational perspectives) and provide an adequate level of privacy protection (the "adequacy" requirement).  
Where the personal data is to be transferred to a processor, such as a cloud service provider, the Directive specifies that the controller and processor must have a written agreement (or legally binding instrument) in place under which the processor undertakes to keep the data secure and to process it only in accordance with the controller's instructions.  
If a breach occurs, the buck stops with the controller as far as the Directive is concerned but a regulator may well inspect agreements between controllers and processors to see if the requirements are being followed. | The obligation to have the 'appropriate organisational and technical measures' in place will apply to both the controller and processor.  
Cloud service providers, therefore, will also be obliged to take such measures when processing data provided by controllers.  
Further, the controller must reserve a contractual right to inspect the processor's facilities. This is something that many service providers have resisted in the past. |
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Directive</th>
<th>Expectations in the Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transferring data outside the EU</td>
<td>Even if sharing is allowed (for example, pursuant to the controller’s legitimate interests), the directive prohibits personal data from being transferred outside the European Economic Area (EEA) unless the controller assures an adequate level of privacy protection (the adequacy requirement). The circumstances in which personal data can be exported outside the EEA are discussed below.</td>
<td>An important change is that the data processor can also be held liable for breaches of the Regulation and not just the data controller. This expands the responsibility to cloud providers.</td>
</tr>
<tr>
<td>Safe jurisdiction (country) list</td>
<td>The European Commission can decide the adequacy of the protection in certain jurisdictions. Transfers of personal data to jurisdictions in the “safe list” are deemed to meet the adequacy requirements. Currently, jurisdictions on the safe list include Argentina, Canada, Israel, Switzerland, Uruguay, Jersey, Guernsey, New Zealand, and the Isle of Man.</td>
<td>The Commission will be able to determine a country, territory, or processing sector in a country or an international organisation as being on the safe list. Only the Commission (not a controller) will be allowed to decide that an adequate level of protection for personal data is in place.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Directive</td>
<td>Expectations in the Regulation</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>US Safe Harbor</strong></td>
<td>Personal data can be exported to the US, which is not on the jurisdiction safe list, if it is transferred to a US company that is a member of the so-called “Safe Harbor” scheme (the company must also adhere to certain principles and make a public declaration to this effect). The Federal Trade Commission administers the scheme, but there is no approval mechanism. It should, however, be borne in mind that US legislation gives US government agencies extensive rights to help themselves to data (including personal data of EU citizens) which is on servers located in the States, irrespective of whether the servers are controlled by Safe Harbor companies. In other words, Safe Harbor status does not guarantee that the data will stay put.</td>
<td>Changes to Safe Harbor were not planned, but reform is now expected following revelations of companies sharing data with the NSA. During 2014, there has been a lot of debate around this area with strong views on both sides. Viviane Reading, the EU commissioner with responsibility for data protection said she had “strong doubts” that Safe Harbor was really safe but said it would be irresponsible to suspend the program. She added that she will conduct a thorough analysis. If the EU decides not to continue to support Safe Harbor, it will create some interesting challenges for US-based cloud service providers.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Today's Directive</th>
<th>Expectations in the Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding corporate rules</td>
<td>Companies with operations in and outside the EEA can use binding corporate rules</td>
<td>These will be approved by a single data protection authority. That said, only larger international organisations are likely to continue to use BCRs.</td>
</tr>
<tr>
<td>(BCRs)</td>
<td>(BCRs) to export data to other companies in their group but that are located</td>
<td></td>
</tr>
<tr>
<td></td>
<td>outside of the EEA. An application is made to the “home” data protection authority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and, if approved, it will be circulated to the other relevant data protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authorities for approval. The rules now include a mutual recognition process in 15</td>
<td></td>
</tr>
<tr>
<td></td>
<td>member states. If the authority receiving the submission accepts the BCRs, other</td>
<td></td>
</tr>
<tr>
<td></td>
<td>participating authorities should do so without further scrutiny. Setting up BCRs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is not to be taken lightly as the documentation must explain how the group will</td>
<td></td>
</tr>
<tr>
<td></td>
<td>provide adequate safeguards and is legally binding; one company in the group has</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to be responsible for the entire group’s compliance; and the entire group has to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>undertake comprehensive data protection audits. In practice, only the larger and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>more sophisticated multinationals choose this option.</td>
<td></td>
</tr>
<tr>
<td>Self-assessment</td>
<td>In the UK, a controller can undertake a “self-assessment” and, if satisfied that</td>
<td>Only the European Commission (not a controller) will be allowed to decide that an adequate level of protection for personal data is in place. This rules out the use of self-assessment in the UK.</td>
</tr>
<tr>
<td></td>
<td>the data will be adequately protected, the data can be transferred outside the EEA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Information Commissioner (the UK’s data regulator) expects any controller to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>be able to demonstrate that an appropriate analysis has been undertaken.</td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Today’s Directive</td>
<td>Expectations in the Regulation</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Model contractual</td>
<td>The company to which the data is to be exported can sign up to model contractual clauses approved by the European Commission. Two sets exist: one applies when the importer is a controller and the other set to when it is a processor. In practice, most companies rely on these clauses to fulfill the adequacy test. Some countries have imposed additional conditions in implementing the adequacy test, such as a requirement to have the arrangements approved by the local regulator before the transfer takes place.</td>
<td>A data protection authority can adopt model data protection clauses that have been declared valid by the Commission or can specifically authorise contractual clauses between the controller or processor and the recipient of the data.</td>
</tr>
<tr>
<td>Other derogations</td>
<td>Personal data can be transferred to countries outside the EU in other circumstances, although these are less likely to be relevant in a corporate context. For example, the transfer can take place if the individuals to whom the data relates have given consent. In practice, however, it is difficult to secure consent from large numbers of people.</td>
<td>No change expected</td>
</tr>
<tr>
<td>Requirement</td>
<td>Directive</td>
<td>Expectations in the Regulation</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Individuals access to their own information</td>
<td>Individuals have the right to demand the information that an organisation holds on them. In the UK, these are known as subject access requests. The data controller is allowed to charge a small handling fee and must respond in a timely manner (in the UK there is a 40-day deadline to respond) - see <a href="http://ico.org.uk/for_the_public/personal_information">http://ico.org.uk/for_the_public/personal_information</a> as an example.</td>
<td>The deadline is expected to be harmonised across the region (with a proposed deadline of 20 days). Individuals will also have a right to erasure - they can contact an organisation and demand that all records are erased (unless this is not technically practicable). This could be tricky to implement, especially in organisations with data stored in many different systems.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Today’s Directive</td>
<td>Expectations in the Regulation</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sanctions and private actions</td>
<td>Failure to comply with the Directive can result in fines, though these are different by country (UK - up to £500,000), negative press reports and a subsequent negative brand image (UK – the Information Commissioner’s Office issues press releases when organisations are sanctioned). To date, the largest fines have been given for serious failures to keep the data secure. The regulator tends to look not only at the individual loss of any data, but the technical mechanisms and training offered to employees together with the scale of the data loss. Individuals can also sue a controller for damages suffered as a result of unlawful processing. This may be rare, but there have been instances of individuals demanding compensation when they received an email from a sender that they didn’t believe had the right to their data. Recent case law arguably makes it easier to claim for distress. The possibility of US-style class action lawsuits being undertaken against controllers also exists.</td>
<td>Sanctions will be tougher. For example, fines will be up to €100m or 5% of global turnover (whichever is higher). However, if the controller or processor has a valid seal (see below), the fine will be imposed only in cases of intentional or negligent non-compliance. The Regulation gives anyone who has suffered damage (including non-pecuniary damage) as a result of unlawful processing the right to compensation by the controller or processor for the damage suffered. Further, the Regulation includes provisions allowing consumer and privacy groups to bring actions on behalf of one or more claimants and there are proposals for collective redress (akin to US-style class actions) in the EU’s legislative pipeline.</td>
</tr>
<tr>
<td>European data protection seal</td>
<td>Not part of the Directive</td>
<td>If both the controller and the recipient of the data have obtained a European data protection seal (discussed below), the adequacy requirement will be met.</td>
</tr>
</tbody>
</table>
### Requirement | Today’s Directive | Expectations in the Regulation
--- | --- | ---
**Transitional periods** |  | Existing adequacy decisions by the Commission (for example, as to which countries are on the safe list) will benefit from a five-year sunset period after the Regulation comes into force and authorisations by data protection authorities (such as transfers based on standard data protection clauses and BCRs) will benefit from a two-year sunset period.

**Informing users and authorities of data loss** | Currently, different countries have different rules on whether users must be informed of data breaches. Breach reporting to supervisory authorities is recommended in all countries and enforced in some. | The Regulation will harmonise the laws on data breaches. Users must be informed if their data is lost unless that data was encrypted. The supervisory authorities should be told within 72 hours of a data breach.

---

**“SENSITIVE” PERSONAL DATA**

There are stronger conditions around sensitive personal data such as racial origin or religious beliefs, and this will continue under the Regulation, (albeit called special categories of data). If an organisation is considering handling such information (or indeed, sharing it) it should take legal advice.

**FURTHER INFORMATION ON THE REGULATION**

The controller or processor may request that its data protection authority, for a reasonable fee, confirms whether the processing of personal data is complying with the Regulation. The authority may accredit specialists to carry out the auditing of the controller or processor on its behalf. If the authority is satisfied that the controller or processor is competent, it will be certified with a seal, which will be valid up to five years. This will be known as the European data protection seal.
The Regulation imposes a general requirement on controllers and processors to carry out and document risk analyses of the potential impact of processing on the rights of individuals. Where the processing operations are likely to present specific risks (for example, if there will be the processing of personal data relating to more than 5,000 data subjects during any 12-month period), the controller or processor is required to carry out a formal “data protection impact assessment” and appoint a data protection officer. Impact assessments must be reviewed regularly (or straight away, if the circumstances change). Although impact assessments are not mandatory under existing laws, the UK’s Information Commissioner has been encouraging their use for some time. Given the potential risks surrounding the user of the cloud, this is an area where documented risk analysis is to be expected.

The Regulation will include all processing by a controller or processor relating to the offering of goods or services to individuals in the EU (irrespective of payment) or monitoring their behaviour even though the controller or the processor is established outside the EU. This means that a US cloud service provider that hosts personal data of EU individuals will be subject to the legislation even if the provider’s clients are not themselves based in the EU. This is new and will mean that a cloud provider also has to conform with the Regulation.

The Regulation introduces a requirement on the controller to notify its data protection authority without undue delay (the current proposal is 72 hours) of any breach of personal data and to inform the individuals concerned. A concern here is that data protection authorities will be inundated with notifications (as there is no materiality qualification) and will not cope. Further, companies remain concerned about having to notify all affected people as a matter of course, not least because of adverse publicity and loss of goodwill.

Personal data is defined widely to include identifiers such as IP addresses as long as they relate to an identified or identifiable individual. The term “sensitive personal data” is replaced by special categories of data that has been expanded to cover gender identity.
Where consent is required, it must be freely given, specific, and “explicit” (whether sensitive or not). Silence or mere use of a service will not suffice. Consent requires clear affirmative action such as ticking a box in a privacy policy. (Presenting users with pre-ticked boxes that they have to untick will not be acceptable).

The Commission had originally proposed a “one-stop shop” for compliance, but this has been replaced by a “lead authority,” where a controller or processor is established in more than one member state or where personal data of residents of several member states are processed. The data protection authority of the main establishment of the controller or processor will be the lead authority and must consult other data protection authorities to reach a consensus. If a consensus cannot be found, the European Data Protection Board (EDPB) must be involved and has the power to impose decisions on the individual authorities.

Under its investigative powers, the data protection authority has access from the controller or processor to all personal data, documents, information, and premises, including any data-processing equipment. A data controller that appoints a processor will therefore need to ensure that it secures the right for the regulator to have access to the processor’s equipment.

CONFLICTING LAWS

There is a possibility of laws from two countries being in conflict. For example, a blind subpoena from the US government may demand data disclosure on an EU individual from a US-based or US-owned entity. In circumstances where EU law requires that the appropriate supervisory body must be informed and prior authorisation needs to be given before the personal data of an EU resident can be transferred to a third party (in this case, the US government), the company may be in the invidious position of having to decide which law to break. (See also the recent case of Microsoft Ireland v US Justice Department⁶, which relates to Microsoft being required to hand over personal data on EU individuals even though the servers are located in Ireland).

⁶ Ruling Against Microsoft Adds to Tech Industry’s Privacy Headaches, Dune Lawrence, August 01 2014 [http://buswk.co/IC3CbsU]
Organisations should not underestimate how easy it is to lose control of data that is in their charge owing to advances in technology and developments in working practices. They need to be on top of the risks to their data and be ready to respond to changes in technology and working practices.

Any organisation which is dealing with personal data should create a team that is responsible for compliance including people with responsibilities for IT, legal, compliance, HR and workers council/employee representatives. It can take many steps for an organisation to conform with the rules, and planning cannot start too early. Security must be made a priority both in terms of the insider threat (e.g. accidental loss of data by employees) and the external threat (e.g. from hackers).

First and foremost, the organisation will need to have its own house in order in terms of security. Technical measures should include installing security software updates as soon as they are available, using robust firewalls to guard against viruses and other malware, and encrypting all mobile devices and storage media to prevent loss or theft of the data.

Organisational measures should include having effective (and user-friendly) policies and procedures in place so that employees and consultants can play their part. Importantly, the policies should be supported by appropriate training, particularly when they are updated. The importance of educating employees about their responsibilities (especially anyone who deals with personal data) cannot be under-estimated.

The data should be checked and different encryption techniques considered depending on the data itself. As an example, there may be call centre employees who need to see some, but not all, of a customer’s credit card information. In this case, techniques may be deployed that encrypt the central six digits while leaving the last four available to confirm the customer’s identity.
Organisations should ensure that strong access control policies are implemented and enforced. For example, the number of people with “super-user” access to the complete data set should be limited and kept under review. Organisations should be keep track of departing employees, and remove their access rights quickly and should look at how to split the data access so that one user cannot access (and potentially lose) too much information.

Anomaly detection technologies should be deployed to identify compromised accounts and insider threats.

It will be worth assessing the extent to which personal data is shared with other group companies or third parties (such as cloud service providers), inside and outside the EU.

Where the data is (or is about to be) shared, the organisation will need to be satisfied that the recipient is also in good shape as far as security is concerned. If the recipient is a processor, such as a cloud service provider, the controller will also need to extract a contractual promise from the processor to this effect. Furthermore, the contractual right to get the data back or have it destroyed should be seen as a minimum requirement. Where the data is to be exported outside the EU, the controller will need to satisfy the “adequacy requirements” (such as having model clauses in place). For example, the use of a cloud service by a processor may, of itself, make the controller non-compliant, particularly if the service provider is located outside the EU and has inadequate security in place.

An organisation should check all contracts that it has with suppliers such as outsourcers and cloud service providers which is processing personal data on its behalf to assess the extent to which the contracts comply with the rules. In addition to the contract, the organisation will also need to be satisfied that the supplier is, in practice, keeping the data secure (e.g. by independent certification or by checking the facilities itself).
The organisation should make itself aware of all cloud services being used by employees, whether sanctioned or unsanctioned by IT. This list should be kept under review and updated on a regular basis as employees can easily start using a cloud service without, say, the IT or compliance department knowing about it. The risk profile of each cloud service should be considered and, where appropriate, closed down (e.g. for high-risk services).

Organisations should also be on top of the use of subcontractors by their suppliers. For example, the use of a Software-as-a-Service typically means that there is a subcontractor sitting behind providing the server infrastructure required to the cloud provider host the software applications. On a related note, it is not uncommon for suppliers to use cloud services without their customers knowing about it, which is a concern in itself particularly when personal data is concerned.

To reduce the likelihood of data loss and to remove or reduce the need to inform users, data should be encrypted when stored by cloud providers. As an organisation could be held liable for data loss by a cloud service provider, it is recommended that the encryption keys are held by the organisation (i.e. the data controller), not by the cloud provider. This can be delivered across multiple cloud services by using a cloud access security broker.

An organisation’s data loss prevention strategy should be extended to cover suppliers such as cloud service providers (e.g. to stop a “comment” field being populated with personal data).

Activity monitoring of access to cloud services should be implemented to provide detailed audit trail for forensics and investigations to identify breaches or high-risk activities.
FIRST STEPS

- Create a team of individuals responsible for compliance. This team should include representatives from IT, legal, compliance, HR and workers council/employee representatives. This team should define the organisation’s policies and ensure that regular reviews are conducted.
- Notify subjects whose data is collected about the purpose of the data collection and ensure that it is possible to share the personal data with third parties.
- Ensure that privacy policies, procedures, and documentation are kept up to date as data authorities can request an audit at any time.
- Create a breach and incident management process that alerts and notifies appropriate authorities.
- Grant subjects access to information about them so they can make any corrections to inaccuracies.
- Review current IT usage, including cloud usage by employees.

CONCLUSION

Any steps an organisation takes to comply with the current Directive and to establish best practice will put it in good stead for the future Regulation. Although the rules can be technical, no organisation should underestimate the importance of applying common sense and taking precautions appropriate to its business and the data for which it is responsible.

Last, but not least, organisations should regularly carry out risk assessments, particularly in respect of activities likely to present specific risks to personal data (such as data sharing). If a company suffers a major security breach, it will not go down well with the regulators if it transpires that a risk assessment has not been undertaken.
FREQUENTLY ASKED QUESTIONS

1. Which countries are in the EU?
The population of the EU is over 500 million people. The 28 countries that make up
the EU are Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic,
Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia,
Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia,
Slovenia, Spain, Sweden, and the United Kingdom.

2. Which countries are in the European Economic Area (EEA)?
The EEA includes all EU countries and also Iceland, Liechtenstein, and Norway. It allows
them all to be part of the EU’s single market.

3. What is the difference between a data controller and a data processor?
Under the EU Directive, the data “controller” is responsible for any data it holds and for
ensuring that the data is “processed” in accordance with the Directive’s requirements.
The controller is the “person” that decides what to do with the data, such as a retailer
holding personal data on its customers. The data processor processes data on behalf
of the controller, so a cloud service provider is an example of a data processor. The
Directive places no obligations on the data processor, however the Regulation will.

4. What is personal data?
Any data that can be used to identify an individual. It has also been referred to as
personally identifiable information (PII).

5. What’s the difference between a directive and regulation?
A directive needs individual country legislation to implement it. Local implementation
has, in this case, led to 28 different sets of laws that are implemented and enforced
differently. A regulation needs no further local laws and should be enforced similarly
across the region.

6. What is the likely timing of the Regulation?
The EU Directive is in effect currently. The Regulation is likely to be finalised in the
summer of 2015 and implemented two years later.
7. Is Safe Harbor at risk?
The US Safe Harbor scheme has been under fire for the last few months in light of Safe Harbor companies co-operating with requests by US government agencies to disclose personal data. The EU Commission Communication, “Rebuilding Trust in EU-US Data Flows” (Nov 2013), made 13 recommendations and initiated a plan to review it. The European parliament called for a suspension of the Scheme (March 2014). However, the new Commissioner for Justice, Individuals and Gender Equality, Věra Jourová, said she is not willing to suspend Safe Harbor at this stage (October 2014).

8. What is the case of Microsoft Ireland v. US Justice Department?
This case concerns personal data also held in Ireland that the US government is demanding that Microsoft hand over. There is a good article about this in Businessweek: http://www.businessweek.com/articles/2014-08-01/microsofts-ireland-data-center-subject-to-u-dot-s-dot-search-warrant-court-rules

9. I am not in the EU – why should I care?
Do you have customers in the EU? The EU data protection regime affects anyone who has data on EU-based individuals wherever the data controller and data processor may be based.

10. Am I responsible for my subcontractors?
Yes. Keep an eye on the extent to which your suppliers use sub-contractors as the same considerations apply. You will be held responsible if something goes wrong.

11. Am I compliant if my cloud providers encrypt the data at rest?
No. Just because your service provider encrypts data doesn’t mean that it will save you from responsibility if that data is then lost.

FINALLY – IT’S NEVER YOUR DATA

One of the major principles of all of the EU data protection legislation is that data kept on individuals by your organisation is never actually “yours.” The data belongs to the individual and they (may) have lent it to you for your business purposes, and just like any loan, they can revoke that right at any time.

To gain visibility and control over the cloud contact Skyhigh Networks today