International Data Privacy Legislation Review: A Guide for BYOD Policies

Enterprise mobility strategy must account for parameters set by local data privacy laws

Reference Code: IT006-000234
Publication Date: 17 May 2012
Author: Richard Absalom

SUMMARY

Catalyst

The spread of smartphones and tablets in the consumer market is having a big impact on the world of enterprise IT, with consumer-focused mobile devices making their way into the organization through the bring-your-own-device (BYOD) trend. IT departments are increasingly realizing that BYOD is happening whether it is officially sanctioned or not, and they are taking steps to address the trend with technology solutions that secure corporate data across a range of platforms and devices.

One important aspect of coping with BYOD that is getting less attention, however, is the impact of employee data privacy legislation and how this creates constraints for IT managers implementing a BYOD policy. Implementing a mobile device management (MDM) solution on a personally owned device will, in most cases, entail a certain degree of activity monitoring and access to data. This can leave the organization in danger of breaching its employees' data privacy rights and therefore open to a lawsuit. Enterprises are therefore presented with a dilemma: they must protect corporate data accessed on an employee-owned device, especially any sensitive customer data, as they will be liable in the event of data loss or misuse, but they must do so without invading the employee's right to personal data privacy.

This report offers guidance concerning privacy laws relevant to BYOD in eight major geographic markets, providing recommendations for and case studies of BYOD implementations. It also provides a framework around which to create a corporate mobility policy that helps ensure compliance with the law while protecting corporate data.

This report is not meant to be a substitute for legal advice. In all cases where an enterprise seeks consent from employees for monitoring an employee-owned device, Ovum recommends seeking local legal assistance. However, this report is designed to make CXOs and IT managers aware of the issues, key questions they should be asking legal counsel, and potential best practice for achieving employee consent and building this into the process of a BYOD policy rollout.

Ovum view

Driven by Apple's and Google's consumer marketing focus, the smartphone and now tablet markets are reaching huge scale. Consumers want to use their mobile devices in all areas of their lives, including at work, so BYOD is happening whether the IT department likes it or not. It is not an issue that can be ignored: aside from the potential benefits of letting employees use their favorite devices, not managing BYOD presents serious data management and security risks.

Requiring employees to sign up to a mobile policy is the best way of ensuring both data security and legal compliance. Installing software on a personally owned device that enables an employer to monitor activities and perform such functions as remote lock and wipe provides a good level of data security but also implies a certain amount of access to personal data. National data privacy regulations invariably state that individuals must give explicit consent for any organization to access and process such data. So making employees fully aware of the implications of bringing their own device to work before asking them to sign a corporate policy and installing an MDM solution on their device covers both bases.

Creating and signing a corporate mobility policy implies a certain level of compromise between the employee and employer. The employer allows employees to use the device of their choice, while the employee recognizes their responsibilities in regard to corporate data protection and allows a certain level of monitoring on their personal device.

Organizations must take national data privacy law as well as vertical-specific regulations into account when developing their corporate mobility policies. There are some differences between data privacy laws in different countries, but two consistent themes apply to all:

- Individuals must give fully informed and unambiguous consent for an organization to access and process their personal data
- Organizations processing sensitive personal data must take adequate technical and organizational measures to protect that data. At a minimum, in the world of BYOD this means that devices must support encryption, either on the device or the communications channel, and the organization must enforce a strong PIN policy.

Key messages

BYOD is the common face of IT consumerization

Mobile consumerization and the trend towards BYOD is happening whether the enterprise wants it to or not. Employees accessing corporate data and applications on personal devices present a huge risk to data security, but attempting to secure data by monitoring personally owned devices can be seen as an invasion of individual privacy rights. Organizations of all kinds face the task of securing their data while also complying with data privacy regulations.

Update the organization's IT acceptable use policy

Requiring employees to sign up to a mobile policy that outlines security measures and the responsibilities of both the employer and the employee is the best way of ensuring both data security and compliance with data privacy regulation. It can also help to set out a framework for managing mobile costs and extracting value from mobile consumerization.

Adopt formal information governance principles

While data privacy laws differ from country to country, two main principles across geographies have an impact on enterprises implementing a BYOD policy: organizations must take adequate measures to secure any personal data that they process; and individuals must give explicit consent for their personal data to be accessed and processed.

Understand and accommodate local privacy laws

Vendors are looking to incorporate the process of achieving employee consent into over-the-air (OTA) device provisioning workflows. Enterprises looking to implement this type of solution should seek legal advice on how this form of consent will hold up against local privacy laws, as it may not be as binding as a signed policy or contract.

MARKET CONTEXT: MOBILE CONSUMERIZATION AND BYOD

BYOD is happening whether IT likes it or not

The smartphone and tablet market, driven by Apple and Google, is taking off and reaching mass in the consumer space. Consumers use these devices in all areas of their lives, and increasingly see the benefits of using them for work purposes – they do not want to carry two devices all the time, one for work and one for personal usage. So, whether officially sanctioned by their employer or not, employees find ways to get around the system and use their personal devices to access corporate applications and data. Towards the end of 2011, Avanade surveyed over 600 executives from organizations in different

verticals across the globe, and 80% reported employees using personal devices at work. Most of this personal device usage is from employees accessing corporate email.

With this trend in mind, BYOD is not an issue that can be ignored, even if the IT department or business leadership does not agree with the idea. Not only would organizations not get any of the potential benefits from BYOD (such as improved employee productivity, engagement and satisfaction, and reduced hardware and maintenance costs), but letting it run unchecked presents serious data management and security risks.

BYOD presents additional data security risk...

Enterprises have faced these kinds of issues before: in many ways BYOD is similar to employees carrying data on USB memory sticks. However, now there is a processor attached to a constantly connected data store, providing a greater range of ways to send, receive, process, and potentially lose data.

BYOD in practice generally means accessing email from a personal device, and this presents risks given the potential nature of data sent by email and how easily a mobile device can be lost – or hacked if not sufficiently secured. Employees accessing corporate data on personal devices present a huge risk to data security unless the correct protection measures are in place.

Businesses embracing BYOD are moving away from an easily controlled, locked-down, homogeneous IT environment towards a multi-platform, multi-device environment. A typical business might have had a fleet of BlackBerrys, managed through the BlackBerry Enterprise Server, and provide desktop and laptop PCs all running on a particular version of Windows. These are all designed with businesses in mind and are relatively easy to monitor and secure. Now it might be faced with smartphones, laptops, Macbooks, and tablets running on iOS, Android, and different variants of Windows – all of which put together are far harder to secure. IT departments can apply an ActiveSync policy that mandates a PIN, but this is the most basic level of security available and still leaves the device open to a mildly determined intruder.

Data loss is the biggest concern, and considering the three main points where threats are present – on the application, on the network, and at the endpoint – BYOD multiplies the number of each of these points. Most organizations are unlikely to have the required tools and expertise to manage and secure corporate data across all these disparate operating systems, applications, and devices.

MDM and enterprise mobility management vendors are jumping in to fill the resultant gap in the market, providing the tools to secure devices and more importantly data. These vendors are of course apt to highlight the worst-case scenarios and create a certain amount of fear among IT managers as part of the marketing strategy, but this does not disguise the genuine need and demand for tools to address the challenges created by BYOD. Typical MDM features include:

- Providing encryption if it is not natively supported

- Remote lock and wipe capabilities for when a device goes missing or falls into the wrong hands
- PIN policy enforcement
- Over-the-air (OTA) device recognition and enrollment
- Device location and activity tracking.

These third-party vendors are experiencing huge growth due the demand created by BYOD, and enterprise mobility management is a very competitive hotspot at the moment. However, while enterprises implementing such a solution may find that it answers their technical problems, installing such software on personally liable devices can create further issues related to employee privacy rights.

...but the solution to the security risk raises issues about employee privacy rights

If sensitive personal data (in the enterprise this might mean client details) is lost, leaked, or misused, the enterprise runs the risk of a fine from the local data regulatory authority. Even if it is lost via usage on a personally owned device, the company is ultimately responsible, not the individual employee. So the enterprise must take measures to protect that data.

However, attempting to secure data by monitoring personally owned devices can be seen as an invasion of individual privacy rights. Across different geographies, data privacy legislation dictates that individuals must give fully informed and explicit consent for their personal data to be accessed and processed. In the practical world of BYOD and MDM, this "access" means monitoring activity and potentially locking and wiping the device – functions that employees may not be too happy about allowing on their personally owned smartphones or tablets.

So organizations of all kinds face the simultaneous task of securing their data while also complying with data privacy regulations – either by gaining employee consent or by managing the data in such a way that it doesn't affect personal data and consent is not required.

Data privacy concerns are at the forefront of the consumer technology debate, but not with BYOD in mind

Data privacy is often in the news, but primarily in relation to its usage by social networks and advertisers, not in corporate mobility scenarios. However, it is a highly important issue for organizations of all sizes, across verticals and geographies. This following sections of this report aim to provide a framework around which to base a corporate mobility policy, as well as outlining the aspects of data privacy law in eight key geographies that may affect enterprises implementing a consumerized mobile policy.

RECOMMENDED CORPORATE MOBILITY POLICY FRAMEWORK

The exact details of a corporate mobility policy that covers both employee- and corporate-liable mobile device usage will differ for every organization. Because it is likely to impact employees at all levels of the organization, it requires input and buy-in from all areas: not just IT but also HR, legal, and line-of-business teams. Policies should also be as short and easily digestible as possible, as they need to be fully understood, relevant, and actionable by all members of the organization.

A corporate mobility policy implies a level of compromise between the employee and employer. The employer allows the employee to use the device of their choice, while the employee recognizes their responsibilities in regard to corporate data protection and allows a certain level of monitoring on their personal device.

The policy should take into account requirements around security, privacy, expense management, and tax, as well as any vertical-specific or locally imposed regulations. As such, individual policies should be drawn up for every different country in which an organization operates. However, to comply with data privacy regulations in the majority of countries, two main principles must be upheld: personal data (for example any client or patient details that an organization is holding) should be adequately secured from loss or misuse; and individuals must give explicit consent for their private data to be accessed and processed.

Because every policy must be unique, the following is not a policy template but a framework of ideas, questions, and considerations around which to build a policy.

Security

The primary purpose of any corporate mobility policy should be to ensure the security of corporate data. There are certain key questions in this regard that should be addressed:

- What basic steps will be in place to ensure device and data security and prevent data loss? (For example, these could include: encryption; PIN enforcement; activity monitoring and logging; device tracking; remote lock; remote wipe or partial wipe; anti-malware and anti-virus protection; individual application protection; document control; or applying limitations to certain applications e.g. turning off the camera.)
- How will these security features be deployed? Are the tools and expertise available in-house or is third-party software required?
- What happens when a device is lost or stolen: Will it automatically be locked? Will it automatically be fully wiped? Will it be selectively wiped to remove corporate data only? Will the corporate data be wiped and the employee given the choice of whether to wipe personal data?
- What happens when the wrong PIN / password is entered too many times: Will the device be automatically locked or wiped?

- What happens when a device is infected with malware? Can it be auto-quarantined, or should it be reported by the user and dealt with by the IT department?

Employee privacy

Implementing any of the security measures discussed above on a personally owned device has a potential impact on an employee's privacy rights. An organization establishing a corporate mobility policy that embraces BYOD should be aware of local legislation in the regions in which it operates, but the following points should be taken into consideration regardless of location:

- Employees should know exactly what will be monitored and/or accessed on their device, i.e. which applications will be monitored and/or eligible to be wiped in the event of the loss of device or the employee leaving the organization. Individuals should be fully aware of the implications of the policy and any management software installed on their device.
- Employees should give explicit consent for any security or access solution (such as an MDM client or corporate app store) to be installed on their device. If consent is not given, the solution should not be applied. Equally, the employee should then be made aware that they may not use their personal device for work purposes – and may face disciplinary action if found to be doing so.
- Even if the security solution is configured to completely ignore personal data and applications, it is a good idea to ensure that the employee understands, accepts, and agrees with this and still require consent to deploy the solution. This may protect the company from any future allegations by disgruntled employees that they did not know what they were signing up for. Of course, if the enterprise claims that it will not encroach on personal data, it must ensure that it does not do so in practice.
- Vendors are looking to incorporate the process of achieving employee consent into the OTA device provisioning workflows, i.e. making it impossible to deploy and use an MDM-type application or environment until the user has agreed to terms online, via SMS or otherwise. Enterprises looking to implement this solution should, however, seek legal device on how this form of consent will hold up to local privacy laws, as it may be as binding as a signed policy or contract.

Eligibility

When considering a corporate mobility policy, organizations should develop a clear idea of exactly who and what it will apply to:

- Will the policy be limited to certain job roles or departments, or will it apply to the whole organization?
- Are different policies required for different employees or departments? For example, will some users be allowed to bring their own device, and will some be restricted to corporate-liable devices? Will some employees not be eligible to use a mobile device at all?

Acceptable use and dealing with policy violations

Once security, privacy, and eligibility concerns have been addressed, businesses need to ensure that the provisions in the policy are adhered to. There should therefore be clearly defined rules around acceptable use and what the consequences are if employees are found to be violating the rules:

- On both corporate- and employee-liable devices, will there be any restrictions or guidelines on Internet usage? For example, will certain applications or types of content be restricted both on work and personal time? Ovum suggests that the lock-down of the PC has been a driver for the use of personally owned smartphones in the workplace, and therefore attempting to impose onerous restrictions on a personally owned smartphone may not be an appropriate solution.
- What happens when there is a violation, e.g. if an employee refuses to sign up to the mobility policy and accept the security provisions but still goes ahead and accesses corporate data on an unsecured personal device? Ovum recommends that disciplinary measures be put in place for employees violating the policy by accessing corporate data without agreeing to the security measures put in place. This is because if they do so and lose data, the company is liable for legal penalties, not the individual. Disciplinary measures should always be a final resort, but an organization has to do what it can to protect itself and ensure that employees help it comply with regulations.
- With the above in mind, Ovum recommends that corporate mobility policies should include an opt-out provision that makes employees fully aware of the consequences of their actions should they then choose to unofficially "opt in" on a non-secured device.

Technical support

BYOD can lead to users being more self-supportive and relying less on the helpdesk, but a mobility policy should clearly define who is responsible for technical support of both corporate- and employee-liable devices:

- Who is responsible for technical support: the IT desk or the individual?
- Will users be responsible for some applications and/or services and IT others? If so, which?
- To what extent are users expected to keep their devices up to date with the latest patches, OS upgrades, etc.? Will the IT desk offer support in upgrading employee-liable devices if asked?

Reimbursement and total cost of ownership

Last on this list, but by no means the least thing for enterprises to consider, is the issue of total cost of ownership and how it impacts their mobility policy. A BYOD policy may not always be a cost-saving exercise first and foremost, but organizations should have an idea of the financial impact of such a policy and establish means to control it. Costs and regulations around tariffs differ from region to region, but the following issues should be considered regardless of location:

- Who pays for the hardware, the employee or the business?
- Who pays for air time / data connection, the employee or the business?
- If the business is paying for the hardware and/or the wireless connection, how will this be addressed: via expenses? Through a stipend?
- Should a hybrid approach be considered, such as letting the employee bring the hardware but supplying a corporate SIM? This option offers two benefits: corporate tariffs are much less expensive per device than paying for a whole range of personal tariffs (especially in Europe); and the phone number remains the property of the company, so when an employee leaves he or she does not take the number and related contact information.
- What are the costs involved in either supporting this policy in-house or bringing in a third-party enterprise mobility solution?

INTERNATIONAL DATA PRIVACY REGULATION RELEVANT TO BYOD

Ovum has identified the relevant aspects of data privacy legislation in a selection of key geographies in order to guide organizations putting together corporate mobility policies for their operations in those regions. As they look to implement solutions that protect corporate data on personally owned devices, businesses can stay on the right side of the law in terms of their employees' privacy by understanding and complying with these pieces of legislation.

Member states of the European Union: proposed data privacy legislation

Employee data privacy

On January 25, 2012, the EU unveiled a draft Data Protection Regulation which, if ratified, will supersede the existing EU Data Protection Directive of 1995 and is also likely to supersede local regulation in member states.

Aspects of European Data Protection Regulation for companies evaluating a BYOD strategy

The principle issue in the proposed regulation is the “right to be forgotten” – for a person to have their profile and data deleted from a website without any difficulty. The regulation is more concerned with privacy on the public web rather than employee-employer relationships, but there are a couple of points that will apply to BYOD.

Chapter 4 Section 2 Article 30 obliges data controllers and processors to implement appropriate measures for the security of processing data, and Articles 31 and 32 lay out an obligation to issue notifications of personal data breaches.

Chapter 4 Section 4Article 35 introduces a mandatory data protection officer for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor (an individual, team, orcompany) consists of processing operations that require regular and systematic monitoring.

Recommendations for enterprises in the EU

"Appropriate measures" should be put in place when handling personal data (about a living, identifiable individual), although the regulation does not specify what this means exactly. It should "ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation." In practice this means that, at a bare minimum, devices handling corporate data should have PIN policy enforcement andAES-128encryptioneither on-device or through the comms channel.

Businesses should appoint an officer to be specifically responsible for any data monitoring and security issues, not just on personal devices but for the organization as a whole.

Germany

Employee data privacy

On August 25, 2010, Germany's federal government approved a new draft law on employee data protection. The planned amendments would apply to essentially all data collected and used by employers over the course of an employment relationship. The scope would not be restricted to automated data processing, so that, for instance, handwritten remarks about employees and personnel files would also – as today – fall under the data protection guidelines. Already, under current law, violating the statutory rules on data protection may in certain events trigger a serious fine or even imprisonment.

In addition, there are data protection regulations that apply to specific areas and that are contained in special laws. Those special laws take precedence over general legislation. Examples include the German Banking Act and the Money Laundering (Prevention) Act, the Telecommunications Act, and the Regulation on the Supervision of the Telecommunications Sector.

Aspects of the German Federal Data Protection Act for companies evaluating a BYOD strategy

Numerous general provisions exist on collection and processing of personal data in the course of existing employment for purposes of the employment relationship (Sec. 32c, 32d D), without material changes to the currently applicable law. The draft bill contains more specific rules on the use of positioning (Sec. 32g D) and biometric (Sec. 32h D) systems.

In relation to telecommunications services that are exclusively used for business purposes, there is a provision (Sec. 32i D) corresponding largely to current practice and case law. The content of telephone calls is regulated more strictly than the content of email and Internet; apart from any monitoring based on actual suspicions, it will only be possible to carry out controls in some limited scenarios.

With respect to private use of telecommunications services at the workplace, the employer is considered to be a telecommunications services provider vis-à-vis the employees and is thus subject to the stricter data protection rules of the German Telecommunications Act and telecommunications secrecy and, hence, may neither access the content of private email communications nor, if no separation can be ensured, of work-related emails.

Solutions proposed center on securing agreements with works councils and individual consents. Employee consents on their own, without works council consent as well, will be invalid.

Recommendations for enterprises in Germany

Businesses considering a BYOD strategy or use of an MDM solution as part of an enterprise mobility strategy must be aware of the complex legal environment in Germany created by the German Federal Data Protection Act.

Provision of services to employees will require sanction by relevant works councils, and specific rules govern the use of positioning technology for any employee or data management purpose.

Tracking and monitoring employee emails, even if work-related and on corporate-provisioned devices, can contravene the Federal Data Protection Act if personal emails are also allowed on the device or account. Implementing a BYOD policy, where personal and work emails are naturally accessed via the same device / account, may therefore involve an organization giving up control over how it monitors employee activity.

Case study: Volkswagen

In December 2011, Volkswagen agreed to deactivate the email function on its BlackBerry fleet at night. Employees in Germany only receive emails from half an hour before the start of flex-time working hours until half an hour after they end, although they can still make and receive phone calls. The move was a result of pressure from the company's works council to counter expectations that the 1,150+ employees with a BlackBerry at Volkswagen's six plants in Germany should be reachable at all times. The works council reasoned that such an addiction to the "CrackBerry"corporate device heightens the risk of burnout and stress, leading to increased numbers of sick days taken. The response to the nighttime deactivation has been very positive within the company.

Case study–based recommendations

Be aware that allowing a BYOD policy or provisioning employees with consumer-focused devices does not automatically mean that they will be reachable at all times.

Organizations implementing any enterprise mobility policy must do so in cooperation and agreement with local works councils. If any such policies do not conform to the employee's contract of employment (e.g. on required working hours), expect opposition from the works council.

UK

Employee data privacy

Regulations on employee data privacy in the UK are covered in The Data Protection Act 1998. Employees should always be made aware of what personal data their employer is collecting, how it is being used, and who has access to it (part 2, section 7).

Aspects of the UK Data Protection Act for companies evaluating a BYOD strategy

The Act doesn't prevent employee monitoring, but it does set out principles for data gathering and acknowledges the employee's right to a certain amount of privacy in the workplace. Employees should be aware of any monitoring that is going on (except in rare cases where there is the possibility of criminal activity), and opening private emails or accessing private data can be construed as a violation of privacy. Employees have a legal right of access to any data that their employer is holding about them.

The Act requires that any adverse impact of monitoring on workers is justified by the benefits to the employer and others. Adverse impacts are justifiable in cases concerning criminal activity, gross misconduct, or health and safety. Any breach of the Act's requirements by an employer that causes damage or distress to the employee can lead to the employee seeking compensation.

Where sensitive personal data is being accessed by a mobile device, adequate security is required to comply with the Data Protection Act (Principle 7: "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"). Encryption is the minimum security standard expected by the Information Commissioner's Office (ICO), which enforces the law.

Failure to put appropriate security measures in place to protect personal data held by the company is a breach of a company's Data Protection Act obligations. So if data is lost via a non-secured employee-owned device, the company and individual officers are liable to be fined rather than the employee.

Recommendations for enterprises in the UK

Businesses implementing a mobility policy that includes BYOD need to at the very least inform employees about exactly which activities will be monitored on their personal devices. The best course of action is to gain consent from employees to access and monitor their devices. Accessing a device in order to wipe data from it implies a certain degree of interaction with personal data, so to do so requires explicit consent from the employee.

Mobility policies should result in a signed contract between employer and employee: The employer should consent to allow usage of personally owned devices at work; the employee should allow the business a specified level of control over the device.

Employees who choose not to sign up to this policy would then still need to be supplied with a corporate-owned device if the business deems it necessary. Forcing employees to use a personal device at work is likely to result in legal challenges. A BYOD policy should therefore be voluntary. If not voluntary, then employees will expect to be compensated for the cost of purchasing and using their own device and/or SIM.

Businesses should ensure that any personally owned device used to access corporate data, which may include sensitive personal information, supports encryption as a minimum security requirement.

Businesses should put all reasonable measures in place to protect against sensitive data loss. If it cannot be proven that appropriate measures are in place, the company rather than the individual involved would be liable to a fine from the ICO if sensitive data were lost through usage on an employee-owned device.

Case study: Leeds city council

Leeds city council is taking the first steps towards a full BYOD policy, allowing staff to choose their own phone, including iPhones and Android devices (although personal laptops are not yet allowed). The council began work on the implementation in early 2012, selecting MobileIron's MDM solution to enable the scheme. Employee's wanting to enroll in the BYOD scheme can only install the MobileIron software after signing a text message disclaimer agreeing to keep their phone updated with the latest OS, apply security updates, and not attempt to circumvent any of the security measures. Once an employee downloads the MobileIron client app, work email, documents, and data are encrypted when accessed on the employee's personal device. At least 130 staff had signed up to BYOD as of April 2012, and the council was considering extending the solution across the city's 270 school sites.

Case study–based recommendations

Make sure that employees are fully aware of what activities and data on their personal devices will be monitored and how. Ask employees to sign up to a mobility policy before allowing them access to

corporate data on their personal devices, outlining their responsibilities in regards to protecting corporate data.

Implement adequate security steps, including data encryption, to prevent the loss or leakage of data through usage on personally owned devices. This may well involve buying into a third-party solution if such capability / expertise is not available in-house.

The “adequate” security steps (i.e. AES-128 encryption) laid out by the ICO should be seen as a bare minimum – from a business and reputational perspective, supporting the bare minimum legal standards will not be regarded as appropriate or satisfactory in the case of a data loss incident.

France

Employee data privacy

French data privacy law was first enacted in Law Number 79-17 of January 6, 1978, which also set up the French Data Protection Authority, the Commission Nationale de l' Informatique et des Libertés (CNIL). Privacy protection during data processing was also covered in theLaw on theRights of Citizens and their Relationship with Administration of April 12, 2000, and the Law on Patients' Rights of March 4, 2002.

The 1978 law was superseded by the Law relating to the Protection of Data Subjects as Regards the Processing of Personal Data (Law Number 2004-801 of August 6, 2004).

Aspects of the Law relating to the Protection of Data Subjects as Regards the Processing of Personal Data for companies evaluating a BYOD strategy

The following parts of the Law are relevant to companies evaluating a BYOD policy:

- Chapter 2, Section 1, Article 6: Datashall be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.
- Chapter 2, Section 1, Article 7:Processing of personal data must have received the consent of the data subject.
- Chapter 4, Article 22, Clause 3: Organizations with a CNIL-recognized personal data protection officer can avoid some of the formalities prior to commencing data processing outlined in the Law.
- Chapter 5, Section 1, Article 34: The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data. Article 34 Prime, Clause 3: Each provider of electronic communication services shall keep an updated record of all breaches of personal data.

Recommendations for enterprises in France

Enterprises implementing a BYOD policy that involves any level of monitoring of an employee's personal device must gain consent from the individual to do so. It is important therefore for employees to sign up to a corporate mobility policy, fully aware of what their employer will be able to access and monitor on their personally owned device.

Organizations should appoint a personal data protection officer to oversee all aspects of data protection within the business, including in relation to BYOD. The role should include keeping track of and reporting any and all data loss incidents or other breaches of personal data.

Organizations implementing a BYOD policy should take reasonable security precautions to protect the data being accessed on personally owned devices. The law does not specify what "reasonable" means exactly, but at a minimumtheenterprise should make sure that devices support encryption and enforce a PIN policy. If an organization is handling a large amount ofdata orparticularly sensitive data, "reasonable" measures may mean taking more precautions such as remote lock and wipe, GPS tracking, and secure web browsers and email gateways.

Because data must "be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed," it is important to prevent sensitive data from being stored locally on a personally owned device and then being forgotten about. Enterprises implementing a BYOD policy should therefore consider document control tools that stop data from being stored locally and can also perform such functions as blocking the ability to copy and paste.

Spain

Employee data privacy

Data privacy in Spain is governed by the Organic Law 15/1999 on Data Protection (LOPD) of December 13, 1999. The regulation concerning its implementation was not approved until December 21, 2007.

The Spanish Data Protection Agency (AEPD) is the public law authority that oversees compliance with Spanish law on data protection and privacy.

Aspects of the LOPD for companies evaluating a BYOD strategy

The following parts of the Law are relevant to companies evaluating a BYOD policy:

- Article 5, clause 1d: Individuals have the possibility to exercise rights of access, rectification, erasure, or objection to any of their personal data being processed.
- Article 6, clauses 1 and 2: Processing personal data requires the unambiguous consent of the data subject. Other legitimate reasons to collect data include when: the process is necessary

for the performance of a contract to which the subject is party; necessary to comply with a legal obligation; to protect the vital interest of the subject; it is in the public interest.

- Article 9, clause 1: The data controller or processor shall adopt the technical and organizational measures necessary to ensure the security of personal data against alteration, loss, or misuse. The state of the art of technology, nature of the data, and risks to which they are exposed should be taken into account when deploying these measures.
- Article 10: Any persons involved in any stage of processing personal data are subject to professional secrecy in regard to the data, even after the end of relations with the owner of the file.

Recommendations for enterprises in Spain

Employees at organizations planning to implement a BYOD policy should be made aware of what data will be monitored on or collected from their personal device, and they have the right to see what kind of records their employer is keeping on them.

Organizations planning a BYOD policy should gain the express consent of employees when applying any software or technology to their personal devices that in any way monitors data and activity on that device. Requiring them to sign a corporate mobility policy ensures that consent is given and proven.

Although Spanish privacy law does not refer to the need for security measures in protecting personal data to be “adequate” or “reasonable,” it is inferred that this is the case. Organizations rolling out a BYOD policy should take the necessary measures to secure data on personal devices, with encryption and PIN enforcement a bare minimum considering the advanced MDM capabilities available today.

Those members of the organization responsible for monitoring personal device usage must remember that they are professionally bound to secrecy and should not share personal details about any employee with anyone who is not directly relevant to the case.

Netherlands

Employee data privacy

Data privacy in the Netherlands is regulated by the Dutch Data Protection Authority (College Bescherming Persoonsgegevens or CBP). It supervises compliance with and application of the Dutch Data Protection Act (Wet bescherming persoonsgegevens or Wbp), the Police Data Act (Wet politiegegevens or Wpg), and the Municipal Database (Personal Files) Act (Wet gemeentelijke basisadministratie persoonsgegevens or Wet GBA).

The Dutch Data Protection Act (Wet bescherming persoonsgegevens or Wbp) came into force on September 1, 2001.

Aspects of the Dutch Data Protection Act (Wbp) for companies evaluating a BYOD strategy

The CBP must be notified of all personal data processing activities (Wbp articles 24, 27, 28, 29, 30, 31, 32, 43).

Legitimate grounds for personal data processing include: the subject giving consent; the process is necessary for the performance of a contract to which the subject is party; necessary to comply with a legal obligation; to protect the vital interest of the subject; it is in the public interest (Wbp articles 6, 8, 16, 17, 18, 19, 20, 21, 22, 23).

Individuals have the right to access data that have been processed on them and to be informed about the way in which these data are used, as well as the right to correction of such data (Wbparticles 5, 35, 36, 37, 38, 39, 40, 41, 42).

Organizations must take "adequate" technical and organizational measures to secure personal data from loss or misuse.The adequacy of the level of security depends on the risks involved in the processing and the nature of the data (Wbp articles 6, 12, 13). The CBP recommends taking into account the state of the art in technology, the costs of implementation, and the risks regarding the processing, nature, and amount of data.

The transfer of personal data to countries outside the EU is subject to additional rules, including that the country concerned ensures an adequate level of protection and that the Dutch Minister of Justice has issued a permit for a transfer or category of transfers of personal data (Wbparticles 76, 77).

Recommendations for enterprises in the Netherlands

Organizations implementing a BYOD policy must notify the Dutch Data Protection Authority (CBP) of any activities that will involve monitoring and processing of employees' personal data.

Organizations should make employees fully aware of the implications of any BYOD program to their personal data, letting them know what will be accessed and giving the employee access to any collected data. Organizations should also gain express consent from employees to implement any software that monitors personal device activity. In practice, this means getting employees to sign up to a corporate mobility policy.

Enterprises rolling out a BYOD program should ensure that "adequate" security measures are in place to protect personal data. The law does not stipulate exactly what "adequate" means, but it does recommend taking the latest technology into account. Making sure that mobile devices support encryption and have a strong PIN policy is a reasonable minimum standard, but where particularly sensitive or a large amount of data is involved, stronger measures such as remote lock and wipe, activity logging, document control, and GPS tracking should be considered.

If using a third-party tool from a vendor based outside the EU to manage and protect data on personal mobile devices, enterprises should ensure that the vendor complies with rules regarding the transfer and storage of personal data outside the EU. International vendors with local operations should be able to comply easily with these regulations.

US

Employee data privacy

The US has no single comprehensive piece of data protection legislation, and what is currently covered in the Electronic Communications Privacy Act of 1986 and the Privacy Protection Act of 1980 (PPA) does not relate directly to the issues imposed by BYOD. In February 2012, the Obama administration proposed a Consumer Privacy Bill of Rights that aims to bring US law more in line with that in Europe and will likely have an impact on BYOD.

Aspects of US Federal legislation for companies evaluating a BYOD strategy

In a case of litigation, whether or not a device is employee-owned means nothing – the court may require forensic reviews of all devices in connection with the litigation. All data on a device, including any personal information, must be made accessible. The Fourth Amendment (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures")applies to mobile devices, but when a warrant has been obtained there is no specific differentiation between corporate- and employee-owned devices.

Certain vertical-specific legislation does have an impact on BYOD. For instance, the provisions of the Health Insurance Portability and Accountability Act do not allow patient data to be stored on a personally owned device.

TheElectronic Communications Privacy Actof1986makes itillegal to intercept wire, oral, or electronic communications, unless the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer (part 1, chapter 119, section 2511). A minimum fine of $10,000 can be imposed on those breaking the law (part 1, chapter 119, section 2520).

From the proposed Consumer Privacy Bill of Rights, the following concepts will have an impact on companies evaluating a BYOD strategy if and when confirmed through legislation:

- Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Consumers have a right to secure and responsible handling of personal data.
- Consumers have a right to reasonable limits on the personal data that companies collect and retain.

Recommendations for enterprises in the US

The current (lack of) broad data privacy legislation in the US means that implementing a BYOD policy is unlikely to have the same ramifications as in organizations based in Europe. However, there are still certain legal aspects to bear in mind.

The proposed Consumer Privacy Bill of Rights, if ratified, will bring the US further into line with existing legislation across Europe. As such, any companies evaluating a BYOD strategy must make fully transparent to employees what data the company will be able to access and monitor on personally owned devices.

Asking employees to sign a mobility policy and thus give explicit consent to a certain amount of activity monitoring can help to protect against any suits arising from the provisions of the Electronic Communications Privacy Act of 1986.

Employees must also be made aware that in the case of litigation they may be required by the court to hand in their personally owned devices for forensic examination.

Organizations also need to be aware of the vertical-specific regulations that apply to them.

Case study: US Army

The US Army is aiming to allow some soldiers and civilian employees to use personal devices at work by 2013. Deputy CIO Mike Krieger is advocating that personnel not directly operating in the field should be able to sign a form that allows the government to put a “zero client” (i.e. one that does not allow any data to be stored locally) on the device and then use that device on the network. The Army is aiming to make a major procurement of virtual mobile client technology before the end of 2012, as well as a new version of the Army's CAC Sleds (Bluetooth readers that work with military smart cards to enable users to sign their mobile devices onto Army networks). The majority of devices brought into work would not need to be ruggedized, and the strategy aims to support multiple operating systems.

Case study: Unisys

In June 2011, Unisys started to roll out a BYOD policy for its employees in the US, with other countries scheduled to follow – a process that will involve examining and complying with data privacy regulations in each separate country. At the time of launch, Unisys VP and CISO Patricia Titus stated that the company "felt that it was necessary to adopt a consumer IT framework that enables the workforce to be more productive." To enroll in the program, Unisys employees must allow a public key infrastructure (PKI) device certificate to be installed on their mobile device, as well as remote wipe software. They must also understand and agree that in the event of litigation against the company, personal devices may be confiscated for unspecified periods.

Case study–based recommendations

Unisys's BYOD rollout provides a great example and blueprint for the issues that organizations tackling the issue in the US should consider. Employees should be fully aware of what activities and data on their personal devices will be monitored and how. Employees should also be aware of the potential ramifications of using their own device at work, including that they risk having the device taken away for forensic examination should a court conduct an investigation into an incident at the company.

Ask employees to sign up to a mobility policy before allowing them access to corporate data on their personal device, outlining their responsibilities in regards to protecting corporate data.

China

Employee data privacy

In 2011, the Chinese Ministry of Industry and Information Technology (MIIT) published draft regulations to govern the collection, use, and transfer of personal data. There is no previous legislation in place to do so. Due to be ratified in 2012, this draft, titled Information Security Technology – Guide of Personal Information Protection, may have an impact on organizations evaluating a BYOD policy.

This regulation is being put in place with the express intention of protecting Chinese consumers. The first draft of the regulation is seen as a general guidebook for companies, and when it is officially ratified is likely to become compulsory and enforceable legislation – but there is no precedent or evidence of how stringently it will be enforced.

Aspects of the Information Security Technology – Guide of Personal Information Protection for companies evaluating a BYOD strategy

The following parts of the proposed legislation are relevant to companies evaluating a BYOD policy:

- Data processors (i.e. people or organizations responsible for handling and processing personal data) cannot collect, alter, transmit, use, block, or erase personal data without the person's consent.
- Depending on the purpose of using the data, the controller also has a duty to keep personal data accurate, complete, and up to date.
- If authorizing a third party to process personal data under its control, the data processor must notify the persons concerned before collection by the third party. Data cannot be transferred without the express consent of the subject person.
- Data processors are prohibited from transferring personal data to a foreign data processor without the express authorization of the law or from the government.

Recommendations for enterprises in China

BYOD is to a certain extent already a reality for most businesses in China – very few companies supply workers with mobile devices (as a cost-saving rather than an innovation measure), so most employees already bring their own. However, these personally owned devices are primarily used to access voice and SMS services, a symptom of China's immature mobile data applications market. (See Ovum'sLarge Enterprise Survey: Mobility in China,October 2011.)

To comply with the potentially forthcoming legislation and as mobile telco service offerings develop and drive higher data usage in the enterprise, organizations implementing a BYOD policy in China are advised to gain employee consent before equipping personally owned devices with lock and wipe capabilities – this inevitably involves accessing, blocking, and erasing personal data.

Outsourcing BYOD security controls to third-party suppliers will also require employee consent. Going to a non-Chinese third-party supplier may prove to be difficult as it requires government authorization. This stipulation in the proposed regulations may have an impact on the ability of international enterprise mobility vendors to operate in China, and thus on the choice of tools available to Chinese businesses.

Australia

Employee data privacy

Data privacy in Australia is governed by the Privacy Act of 1988, which has gone through numerous amendments since it was first enacted, most recently in 2011. The Office of the Australian Information Commissioner (OAIC) is responsible for monitoring technological developments that impact data privacy, making recommendations for policy changes, and enforcing the Privacy Act.

Aspects of the Australian Privacy Act for companies evaluating a BYOD strategy

The Privacy Act includes 11 Information Privacy Principles (IPPs), including the following:

- IPP 2: Individuals should know what information is being collected and how it is being used.
- IPP 4:Personal information must be stored securely to prevent its loss or misuse.
- IPP 5–7: Individuals should be able to access the information held about them and correct or amend it if necessary.
- IPP 8–10: Personal information can only be used for a prescribed and relevant purpose, or for another purpose in special circumstances, such as with the individual's consent or for some health and safety or law enforcement reasons.

Recommendations for enterprises in Australia

Businesses implementing a mobility policy that includes BYOD need to at the very least inform employees about exactly which activities will be monitored on their personal devices. The best course of action is to gain consent from employees to access and monitor their devices.

Mobility policies should result in a signed contract between employer and employee, with the employer consenting to allow usage of personally owned devices at work and the employee allowing the business a specified level of control over the device.

Businesses should ensure that any personally owned device used to access corporate data, which may include sensitive personal information, supports encryption as a minimum security requirement. Exact requirements for secure storage are not laid out in the Privacy Act, but it is made clear that data should be secured "by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification, or disclosure, and against other misuse." More stringent security controls should be put in place if a high volume of personal data is being stored or if the data is of a particularly sensitive nature.

Case study:VMware study and SAP

VMware conducted a survey of employees across 10 Asia-Pacific countries, including 200 workers from Australia, and found that over 50% felt they could work more efficiently in a web-based environment on a device of their choice. However, 79% of the firms involved did not offer any support for employees who used their own devices.

SAP's Australian operation has initiated a BYOD policy, which is helping to attract new workers who prefer using their own devices over the corporate-supplied desktop or laptop. In 2011–12, 80% of new hires, mostly in their 20s or 30s, chose to take up the BYOD policy. SAP had planned to roll out a corporate-wide BYOD policy but found that local regulations required it to be implemented on a country-by-country basis.

Case study–based recommendations

The demand for BYOD among younger workers in Australia is not being met by the majority of firms. International firms that are implementing a BYOD policy are seeing the benefits to recruitment.

Multinational businesses that are rolling out BYOD policies understand that it cannot be done on a corporate-wide basis but must be managed according to the privacy regulations in each country in which it operates.

Employees wishing to use their own devices for work should literally "sign up" to a BYOD policy that lets them know what activities will be monitored and clearly outlines the potential consequences, such as data (including personal files) being remotely deleted in the event of a data security threat.

APPENDIX

Further reading

The BYOD Gap: Trends, Strategy, and the State of Mobile Device Management, October 2011

Solutions Guide: Enterprise Mobile Device Management Vendors, March 2012

Methodology

- Ovum conducted extensive desk research into data privacy legislation in the European Union, Germany, the UK, France, Spain, the Netherlands, the US, China, and Australia to uncover the details relevant to corporate mobility policies covering BYOD.
- Information and opinion around the causes of the MDM trend and the security solutions designed to help enterprises deal with it is based on research conducted for the two reports outlined in the "Further reading" section above.

Author

Richard Absalom, Analyst, Consumer Impact Technology

richard.absalom@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.