BYOD: Bring Your Own Device

Employment and privacy law issues

Employment issues

What employment issues must companies consider in deciding whether to switch to the bring your own device (BYOD) model?

Switzerland

Walder Wyss

Employment contracts and BYOD policies

As a rule, employers must provide their employees with any devices that they require for professional purposes, unless the parties agree otherwise (Article 327(1) of the Federal Code of Obligations). Therefore, a BYOD model may be introduced only with the consent of each employee concerned. Consent is considered valid only if it is given freely after adequate information has been provided. If a BYOD model is introduced, a BYOD policy must be set out under the employment agreement.

Before implementing a BYOD model, employers should verify whether any standard or collective employment contracts apply and, if so, whether they contain provisions which are relevant in this context. In addition, elected employee representatives may need to be consulted.

Rules for device use

The statutory framework on employment relationships in the Federal Code of Obligations contains some general rules which apply to the use of devices within a BYOD model. In particular, employees have a statutory duty to safeguard confidential information obtained during (and to a certain extent after the termination of) the employment relationship (Article 321a(4) of the Federal Code of Obligations). Moreover, any data processing by an employer must remain within the limits of Article 328b of the Federal Code of Obligations. According to this provision, employers may only process employee data that:

- concerns an employee's suitability for his or her job; or
- is necessary for the performance of the employment agreement.

It is recommended that any specific employee or employer rights and duties in connection with the BYOD model be clearly set out in the BYOD policy under the employment agreement. In particular, the BYOD policy should contain rules on:

- data security, such as prohibiting third parties (eg, family members of an employee) from accessing the device;
- private use of the device during working hours;
- the separation of professional and private data on the device (technically and logically);
- how employees or the employer can terminate the BYOD use policy;
- software and apps stored on the device (eg, security software and rules preventing the installation of types of software or apps which could cause security risks);
- employers' right to access private devices remotely (eg, to wipe professional data in case of termination of the BYOD use policy); and
- the conditions under which an employee may be obliged to return his or her device so that his or her employer can access the data stored therein (eg, in case of internal investigations).

Compensation

Employees are entitled to appropriate compensation for the professional use of a device unless agreed otherwise (Article 327(2) of the Federal Code of Obligations). Compensation typically covers the actual cost of professional phone calls and internet use for work-related purposes, as well as general use of the device for work-related purposes over time (ie, *pro rata* compensation). It is possible to deviate from this standard by mutual agreement. However, a significant amount of compensation would be considered a hidden salary payment for tax and social security purposes. A lump sum payment is possible as long as the compensation more or less reflects the costs of work-related use of the device (ie, market price or arm's-length compensation).

Working hours and holiday allotments

Under Article 328(1) of the Federal Code of Obligations, the employer must:

- protect employees' personality rights;
- have due regard to employees' health; and
- ensure that proper moral standards are maintained.

Contributors

SWITZERLAND
Walder Wyss

walderwyss

Jürg Schneider

Legal updates

SWITZERLAND
Walder Wyss

walderwyss

Monique Sturny

Legal updates

The Federal Employment Act and Ordinance 3 to the Employment Act contain more detailed rules on the protection of employees' health and work and rest times. The Employment Act and the ordinances thereto apply to most employees in Switzerland. However, some exceptions apply – in particular, the rules on work and rest times do not apply to leading top managers.

The use of a BYOD policy may raise questions as to whether rules on holiday time and, within the scope of the Employment Act, rules on maximum working hours are observed. As an employee will have his or her device always on hand and possibly in constant use, there is a risk that he or she will regularly work outside and in addition to his or her regular working hours. If the employer tolerates excessive use of the device for professional purposes, it may have to provide additional salary. The same applies to the excessive use of a device for professional purposes during an employee's holiday allotment. In this case, the employer may have to grant additional holiday, which can be converted into a compensation payment if the employee has holiday credits at the end of the employment relationship. Further, in accordance with the Employment Act, working at night and on Sundays is, in principle, prohibited and requires special authorisation. Hence, employers should set out clear rules relating to the timeframe within which devices may be used for professional purposes.

Liability
The general liability rules applicable to employment relationships also apply to BYOD.

The employer has a general duty of care with regard to employees and their valuables (Article 328(1) of the Federal Code of Obligations). Thus, employers are liable for any damage to or loss of a device in the workplace that they wilfully or negligently cause (eg, damage of the device due to a virus on the employer's network). In contrast, employers are not typically liable for any damage to or loss of a device that occurs outside the workplace due to a lack of causation.

On the other hand, employees are liable for any loss or damage that they wilfully or negligently cause (Article 321e(1) of the Federal Code of Obligations) – for example, where the employer's computer network is infected with a virus originating from a private device or a third party gained access to company information because an employee lost his or her device.

Back to top

Are there any specific issues that organisations with a global presence, or those in highly regulated sectors, should bear in mind?

Switzerland

Walder Wyss

No specific rules relate to the implementation of a BYOD model in organisations with a global presence or in highly regulated sectors. However, certain sector-specific secrecy obligations (eg, Swiss banking secrecy, medical secrecy, attorney-client privilege and official secrecy obligations) may pose particular challenges when implementing a BYOD policy. Among other things, any unauthorised access to protected information on the device must be prevented. This requirement relates not only to business data on the device containing secret information, but also to secret private data stored on the device (eg, communications between the employee and his or her physician or communications between an employee and his or her personal attorney).

Generally, the international reach of global organisations will raise issues in connection with data transfers abroad. In case of disclosures of personal data abroad (eg, if employee data is being stored on a server located outside of Switzerland), the specific requirements for cross-border data transfers must be met. The Federal Act on Data Protection prohibits disclosures of personal data abroad if such transfer could seriously endanger the personality rights of the data subjects concerned. This may in particular be the case if personal data is sent to a country which has an inadequate level of data protection. Countries that have implemented EU Directive 95/46/EC are considered to provide an adequate level of data protection with respect to data relating to individuals (but in most cases not with respect to data relating to legal entities, which are also protected under Swiss data protection law). For data transfers to non-EU or non-European Economic Area countries, it is necessary to check in each individual case whether the country has an adequate level of data protection. Disclosures of personal data to countries that have an inadequate level of data protection are lawful only under the conditions outlined in Article 6 of the Federal Act on Data Protection. Among other things, such data transfers are lawful if contractual safeguards (typically EU model contract clauses adapted to Swiss law requirements) ensure an adequate level of protection abroad.

Back to top

Privacy and confidentiality

How do privacy laws, employment laws and protecting a company's confidential information overlap or intersect on this issue – and how can they be reconciled, given their disparate aims?

Switzerland

Walder Wyss

Privacy laws, employment laws and protecting a company's confidential information must be considered when implementing a BYOD model. However, these considerations can be reconciled, as their aims are not necessarily disparate.

On the one hand, employment law contains various provisions aimed at protecting employees' personality and privacy rights and the company's confidential information. Among other things, employment law limits any processing by the employer of data:

- concerning an employee's suitability for his or her job; or
- necessary for the performance of the employment contract (Article 328b of the Federal Code of Obligations).

Further, employment law stipulates a duty of confidentiality for employees with respect to a company's confidential information.

On the other hand, the general data protection principles set out in Article 4 *et seq* of the Federal Act on Data Protection and the duty to protect personal data against unauthorised processing through adequate technical and organisational measures (Article 7 of the Federal Act on Data Protection and Article 8 *et seq* of the Federal Data Protection Ordinance) apply to BYOD models and employment relationships in general.

The implementation of a BYOD model may raise concerns as to the protection of a company's confidential information. In particular, the private use of the device may create a risk to the company's business and manufacturing secrets. Further restrictions may apply in specific sectors, such as banking secrecy or medical secrecy obligations.

The federal data protection commissioner recommends implementing specific measures to reduce privacy risks when implementing a BYOD model.

Back to top

For those that make the switch to BYOD, how can the confidentiality of both employer and employee be preserved?

Switzerland

Walder Wyss

The federal data protection commissioner recommends implementing specific measures to reduce privacy risks when implementing a BYOD model, including:

- establishing a policy (a separate BYOD policy or an annex to the respective employment agreement) delimitating, among other things, possible uses of the device and establishing regulations addressing access to the device by the employer;
- maintaining a separation of professional and private data (technically and logically);
- employing data security measures, either through passwords or encryption;
- clearly defining where business data is being stored and preferably storing it on a local server; and
- designating a person to be responsible for approving employee devices.

These measures protect both employees' personal data and the company's confidential information.

Back to top

Separation and ownership of data

Data

How can companies separate out what information sent or received on the device is official and business related? Who owns this information – the employer or the employee? And how can employer access to information be assured?

Switzerland

Walder Wyss

Separation and access
The federal data protection commissioner recommends that business data and private data be separated (technically and logically). There are several options to achieve this separation.

One method is to grant employees only remote access to company data, which is stored in a central location by the employer (eg, company server or cloud provider), not locally on the device. Alternatively, companies may allow local storage of company data. In this case, the use of software tools enabling the storage of company information in a

separate encrypted container on the employee's device is strongly recommended in order to ensure the separation of professional and private data. This approach will also enable the employer to access company information and install security software to the extent required to protect company information while not accessing employees' private files.

Another alternative is to run private and company data on separate virtual machines on the private device (ie, by separating the data on the operating system level (see "Overview on Consumerisation and BYOD", published by the German Federal Office for Information Security on July 31 2013). Although this paper is by a German authority, it can be used as a source of inspiration for BYOD programmes in Switzerland (a link to this document can be found on the federal data protection commissioner's website).

Employers' access rights should be specified in the BYOD use policy. It is highly recommended to obtain employees' written acceptance of the use policy.

Ownership
The employer owns all company-related information stored on the device and is responsible for implementing appropriate security measures to protect this information.

Back to top

Breach events and departing employees

Handling a breach

What happens in the event of a security breach? Is the employee protected from liability?

Switzerland

Walder Wyss

No explicit federal statutory obligation requires data controllers or service providers to report data breaches to the data subjects concerned, the federal data protection commissioner or other public or regulatory authorities.

The Swiss legal doctrine argues that affected data subjects must be informed by data handlers about serious data breaches (eg, unintentional disclosure of personal data to third parties) based on the principles of transparency and good faith. In exceptional cases, these principles may require data handlers to report a serious data breach publicly.

A duty to notify affected data subjects of any data breaches may also arise based on contractual obligations, or due to data security considerations and the general duty to minimise potential damage.

Data breach notification duties (with regard to authorities and possibly data subjects) may be introduced in the pending revision of the Federal Act on Data Protection. However, details are not yet known and, realistically, the revision is not expected to enter into force before 2018.

Employees will generally not be personally liable *per se* for data breaches with regard to third parties. However, they have a duty to inform their employer if their device is lost or damaged or if they are aware of an unauthorised access or other data breaches relating to company data. In addition, if the data breach is the result of inadequate handling of the device and a violation of the employee's general duties of care and loyalty, such conduct may constitute a breach of the respective employment contract. As such, employees' reporting obligations in this respect should be set out in the BYOD policy. For the sake of clarity, it is up to the employer (not the employee) to inform data subjects about a data breach relating to company data.

Back to top

Handling leavers

What steps can a company take to prevent an employee leaving the company from taking company confidential information via his personal device? And how can the employee's own personal information be safeguarded in the process?

Switzerland

Walder Wyss

Employees have a general duty of confidentiality not to exploit or reveal confidential information obtained while in an employer's service (eg, business or manufacturing secrets). Employees remain bound by this confidentiality obligation even after the employment relationship has been terminated, to the extent required to safeguard the employer's legitimate interests (Article 321a(4) of the Federal Code of Obligations). However, an explicit duty of confidentiality is recommended in the respective BYOD use policy. Obtaining employees' written acceptance of the use policy is strongly recommended.

If the employer grants only remote access to company data and this data is stored centrally (on a company server or cloud provider on behalf of the employer), a mere refusal of access should be effective to prevent any company information from remaining on the personal device, as it is not stored locally. Where company data is stored locally on the private device but separated with container software, employers should be able to wipe any company data stored on the corporate side of the device. Doing so should not affect any private data stored on the device, as such data is not integrated with company data.

Back to top