SQUIRE SANDERS

PITFALLS OF USING A COMPANY PHONE FOR PRIVATE PURPOSES

For an employer, the easiest way to deal with an employee's use of a company phone is to restrict him to business use only and not allow its use for private purposes. If the employer approves the use for private purposes, there can be tax implications as well as the increased risk that the employer may be able to access the employee's private correspondence. Moreover, there is a risk that the device might be used by third persons including the employee's family members.

Because of this, the employer should set the conditions for use of the device by the employee as well as the procedures regarding access to the device by the employer. If the employer gains access to the employee's personal data, subject to the regulation under the Act on Protection of Personal Data, they may (if authorization was not obtained) inadvertently interfere with the employee's right to protection of his privacy, which might result in criminal-law consequences. The Office for Protection of Personal Data is very strict in relation to employer access to the content of employees' work e-mails or phones. The right to protection of employee's privacy at workplace is also expressly anchored in the Labor Code. The Labor Code forbids the employer to keep in an employee's personal file any data that is not necessary for performance of the employee's work, under any circumstances.

It is generally very difficult to base any activity of employer on employee consent. In the case of any employee consents or agreements, the employer must keep in mind that the Labor Code does not allow any deviations from its provisions to the detriment of employee. Moreover, from the view presented by the new Civil Code, the employee is considered the weaker party.

Of course, the general prohibition to monitor employee email or phone contents also applies where the employer does not allow the employee to use the phone and/or email for private purposes. This is because, according to the Office for Protection of Personal Data, the employer is not effectively able to prevent a third person from contacting the employee via these means in a private matter, regardless of whether the employer has the employee's private content or not.

Employer's SIM in a Private Phone

Other issues arise where an employer allows the employee to use their own personal device for work purposes, but provides the software and/or SIM for the device. This approach – called BYOD (Bring Your Own Device) – represents even more risks for the employer and, in general, it is not recommended. However, there is no doubt that in certain working situations it can actually be a benefit. In these instances, in addition to the overall security risks and costs of connection and synchronization between the device and its software with the employer's devices and software, it is necessary to keep in mind a few things:

1. The employee is entitled to claim compensation for using his own device for work purposes. This entitlement is stipulated in the Labor Code and cannot be excluded by contract.

2. Some license agreements do not allow installation of software in devices that are not owned by the employer. Moreover, the license agreements may stipulate other restrictions, e.g., forbidding the installation of competitors' software in the same device etc.

3. The employer is not the owner of the device. Therefore, if it does not have remote access to the work applications installed in the employee's device, in practice it cannot (regardless of any contractual provision with the employee) efficiently make sure that, for example, in the case of termination of employment, the employee deletes the employer's content or transfers it to employer's another device. The same also applies to the employer's access to the documents or the results of the employee's work saved in the device. Therefore, the employer may totally lose the control over its own content that is stored in the employee's device. Moreover, in the case of any confidential content, the employer faces the risk that it will forfeit the trade secret protection for any content stored in such device – the loss of control may lead to the conclusion that the employer failed to reasonably secure confidentiality of the trade secret information, which is a precondition for creation of statutory protection of trade secrets.

4. If the employer has a remote access to applications in the employee's device, they must ensure they do not accidentally delete any documents and/or software belonging to the employee. If this happens, the employer may be liable for damages.

The situation represents a smaller risk if any and all applications and data run in cloud services, and are therefore not stored long-term in the employee's device. However, even in this case the employer is still obliged to compensate the employee for using his own device for work purposes. Furthermore, if the employer has not technically disabled copying of the employer's content by the employee from the cloud to the employee's device, the risk of loss of control over its content remains. The market keeps gradually developing mobile devices that enable parallel running of two completely separated operation systems, and in the future this should ensure protection of privacy in using devices for both work and private purposes.

The conditions for using devices, whether owned by the employer or employee, for work purposes should in any case be described in detail in the contract between the employer and employee or in the employer's internal regulations. Respect to the employee's privacy is a matter of fact in this case. Although the employer might feel tempted to look at the employee's private content in the device, which might very easy, it must not do so under any circumstances. It could face private-law recourse from the part of the employee and/or also proceedings at the Office for Protection of Personal Data as well as the work inspectorate authorities, and even a criminal prosecution.

What Else Should Employees Be Aware Of?

- In first place, employee should be acquainted with the conditions for using the device stipulated in the contract with the employer or in the employer's internal regulations.
- The employee should observe the employer's security rules, including the rules on regular replacement of passwords etc., and make a reasonable effort to prevent any data leakage from the device provided to the employee. However, the same also applies to the employee's devices used by the employee for performance of the work.
- In addition to other obligations, the employee should never download or store in any other manner any illegal content in the device owned by the employer. In doing so, the employee could, among other things, induce the employer's liability for breaching rights of third persons.
- Employee should not install any software in the employer device without the employer's consent.

Legal Connections Of Data Synchronization and Updates:

- For synchronization, in the case that employee uses the device for both work and private purposes, it is necessary to strictly separate the private content from the work content and prevent that content getting into the hands of the employer.
- Alternatively, if the employee synchronizes data between work device and his private device, he risks being liable for data leakage as his own device might not be protected in the same extent as the employer's device.
- Updating and synchronizing relates to the employer's attitude to the device. For issues regarding remote access and inability of remote access see the main text of this article.

Author: Lenka Kolarikova, registered legal trainee, Squire Sanders

Published: Právní rádce 10/2013