Privacy Flash

March 2020

Home office: What employers should bear in mind

You might have read our newsletters regarding the declared state of emergency or summarising the impacts of the COVID-19 pandemic on employers. One of its many effects is the mass transfer of the population capable of work to home office – or work-from-home mode. However natural this may sound to some of us, and however unimaginable this may be in some operations, we are experiencing unparalleled use of this mode of work. Plenty of you are now dealing not only with the technical equipment but also the legal issues related to working from home, the provision of information on the employees' health in order to organise their work, data storage in the cloud and the creation of a virtual workplace. In addition, a lot of IT companies have responded to the new situation by offering videoconference software solutions free of charge.

However, when – often hastily – organising work (which is entirely natural given the similar fashion of introducing emergency measures on the government level), companies are forgetting aspects of personal data protection, which have not ceased to apply as the pandemic unfolds. Even such an extraordinary situation requires compliance with laws, including the GDPR, if we do not wish to wake up after the crisis with even greater concerns than with those directly or indirectly caused by the SARS-CoV-2 virus wreaking havoc. This is a fact also confirmed by the European Data Protection Board in its statement.[1]

Let us take a look at nine practical recommendations for secure work from home.

Issue no. 1: Lists of employees in quarantine or a list of infected employees

The processing of information on an employee's health constitutes the processing of a special category of personal data under Article 9 of the GDPR. The employer may process such information for the purpose of carrying out obligations under employment and social security law [Art. 9(2)(b) GDPR]. In addition, under Section 101 of the Labour Code, the employer must ensure its employees' health and safety. That is why the employer may keep records of employees with coronavirus symptoms or those quarantined after returning from risk areas. However, the employer may not disclose lists of these employees but may only inform about the total number of employees in quarantine.

Issue no. 2: Demo versions and software for videoconferences, shared workplaces and cloud solutions free of charge

Before accepting an offer from IT firms, a company should weigh up several aspects: (i) what the overall design of the offered solution is: where the servers are, where the data are stored, who has access to the data and from which places the IT firms provide technical support. The storage space is often in the cloud and the servers are located around the world, with access secured by entities outside the EU. A company using such a solution is responsible for ensuring the lawfulness of the transfer of personal data to a third country, often without knowing that such transfer takes place; (ii) employees should only be able to connect to a videoconference via VPN (Virtual Private Network), in particular, if confidential information is to be discussed, a VPN ensures that the transfer of data shared during the session will be secure; (iii) uploading files to a videoconference programme, which is used on a temporary basis, should be disabled if you do not check where exactly the data are stored and who has access to them; (iv) the same applies to potential videoconference recordings.

Issue no. 3: Recording videoconferences

One of the key principles laid down in Article 5 of the GDPR is transparency. Under this principle, teleconference participants must be informed in advance, ideally already in the invitation to the teleconference, that the calls will be recorded. Participants who do not wish to be recorded while asking a question should be allowed to ask it in advance in the form of an e-mail or chat. All participants need to be informed about the recording at the beginning of the videoconference. Besides that, specific rules need to be set as to (i) which teleconferences may be recorded and for what purpose, (ii) where the recordings will be stored, (iii) who will have access to the recordings, and (iv) how long they will be retained.

Issue no. 4: How to share documents and folders

Employees often need to share large sets of data. To ensure that not only personal but also confidential business data are secured, companies need to set a method for sharing sets of data while avoiding their sharing through free repositories that are not sufficiently secured. Recommended solutions include shared discs or cloud solutions with restricted access (accessed using login and password). Sending instructions to employees via e-mail would be sufficient, provided there is a 100% certainty that employees will follow them, which is not always the case. The only way to prevent unauthorised sharing of data is to prevent employees from accessing the repository websites, i.e. selected websites will be blacklisted.

Issue no. 5: Moving folders

Certain work may entail work with hard copies of documents. Employees should minimise the need to move paper documents. If they need to take some documents home with them, employees must be cautious in handling the documents containing personal data to prevent their

[1] https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en.

Privacy Flash

March 2020

loss while using public transport, or prevent their children from playing with them. Employees should always consider whether it is not safer to finish their work quickly at the workplace than to risk losing the documents, and thus possibly violating Article 32 of the GDPR.

Issue no. 6: Checking employees working from home

Employers have legitimate reasons to check their employees or allocated agency employees working from home. They may check their employees via phone, various software applications that monitor time spent at the computer, or chats monitoring inactivity of the users. In order to fulfil the transparency principle, employers must notify their employees of these checks. It is not possible to install software monitoring the time spent at the computer on employee computers without their being aware of it. On the contrary, it must be clear to employees how their working hours are recorded when their standard arrival to/departure from the workplace is not possible. At the same time, it is necessary to avoid making premature conclusions when using these automated methods – where the employee does not permanently work with the computer, given the nature of the work, but instead can for example study paper documents, then inactive chat or a switched-off laptop cannot serve as the grounds for an automatic complaint that the employee is not working (unlike, for example, a call centre employee where such a link is obvious). It is also recommended to determine who will be authorised to check on employees (authorised employee) and what measures he / she can adopt vis-à-vis other employees. Unless employees are sufficiently informed, the information on non-performance of work tasks cannot be used as the reason for taking corrective action against the employee (e.g. complaint).

Issue no. 7: Phishing

Unfortunately, the number of phishing attacks has not dropped even during the emergency situation. Quite the contrary, with the decline in economic activity and the potential decrease in the number of business e-mails, employees tend to click on alluring links in an e-mail or log in to fake websites. Companies are also urged to be cautious by the Office for Personal Data Protection[2]. Employers should appeal to employees for increased caution and increase firewall protection to reduce the amount of phishing e-mails reaching employees. If the company has an e-learning system in place, this period of lower activity can be used for employee education, including that on computer security.

Issue no. 8: Security incidents

The loss of a folder or unauthorised access to personal data under a successful phishing attack may fulfil the definition of a data breach pursuant to Article 33 of the GDPR. In that case, the employer is obliged to inform the Office for Personal Data Protection within 72 hours from the moment the employer learnt about the incident or the moment the incident occurred. It is worth reminding all employees of the rules regarding secure handling of (not only personal) data because work scattered outside the employer's premises and the usual area of the secured server increases both the risk of an incident itself and its later detection. At the same time, employees should not be afraid to inform their employer of a possible incident and the employer should then consult their data protection officer or lawyer.

Issue no. 9: Sanctions

Setting rules without sanctions is often ineffective. It is recommended to set rules for working from home in an internal regulation pursuant to the provisions of Section 305 or Section 306 of the Labour Code, which also provides for possible sanctions in the event of non-compliance. The policy must be tailored to your organisation and your employees, e.g. in the case of operators, remember to lay down that when answering calls they should be in a separate room without their family members present, and that they should take printed documents back to the company for secure destruction as soon as it is possible; locking one's computer screen should also be a matter of course when working from home.

[2] *On 19 March 2020, the Office for Personal Data Protection shared the following article: https://www.novinky.cz/komercni-clanky/clanek/podvodne-e-maily-zneuzivaji-aktualni-kauzy-cilem-jsou-vase-data-40316964.*

Authors:
Robert Nešpůrek | *Partner*
Richard Otevřel | *Counsel*
Jitka Soukupová Ivančíková | *Legal Expert (FairData)*



HAVEL & PARTNERS

CONNECTED THROUGH SUCCESS

Our team

220 lawyers and tax advisors | **400** employees

Our clients

2,000 clients | **100** of the Fortune 500 global companies
50 companies in the Czech Top 100 league | **7** companies in the Czech Top 10 league

International approach

Legal advice
in more than **90** countries of the world
in **12** world languages
up to **70**% of cases involve an international element

www.havelpartners.cz

PRAGUE
Florentinum, Reception A
Na Florenci 2116/15
110 00 Prague 1
Czech Republic
Tel.: +420 255 000 111

BRNO
Titanium Business Complex
Nové sady 996/25
602 00 Brno
Czech Republic
Tel.: +420 545 423 420

BRATISLAVA
Zuckermandel Centre
Žižkova 7803/9
811 02 Bratislava
Slovak Republic
Tel.: +421 232 113 900

PILSEN
Nepomucká 144
326 00 Plzeň
Czech Republic
Tel.: +420 371 005 320

OLOMOUC
Salm Palace
Horní náměstí 371/1
779 00 Olomouc
Czech Republic
Tel.: +420 581 000 310

OSTRAVA
Smetanovo náměstí 979/2
702 00 Moravská Ostrava a Přívoz
Czech Republic
Tel.: +420 255 000 111