TUCA ZBARCEA
ASOCIATII

14 April 2020

# COVID-19 Legal Insights

**In this issue:**



## Cybersecurity recommendations for organisations using remote work systems

EUROPOL has recently announced that the number of cyberattacks against organisations and individuals significantly increased in the context of the COVID-19 endemic. The information provided below is mainly based on the views expressed recently by EU data privacy regulators and by the European Union Agency for Cybersecurity (ENISA).

### 1. What controls can employers put in place to protect their information in the context of remote work?

In order to protect their information in the context of remote work, employers can implement measures at the level of the organisation, as well as technical measures, as highlighted herein below.

**a) Organisational measures**

- To regularly inform their staff on how to react if they encounter difficulties in using remote work tools (e.g. authorised personnel that they can call, hours of service, emergency procedures).
- To ensure adequate support for staff encountering difficulties in using remote work tools. This may require setting up special schedule for the staff.
- To restrict the Internet access from remote access protocols (and other potentially vulnerable protocols) if such access is not needed.
- To ensure that the employees are fully aware of the remote access procedures (for example, VPN, multi-factor authentication, etc.).
- To ensure that all employees can be contacted at any time and that they are fully familiar with the communication channels.

- To restrict access to systems that require special protection. For example, the staff connectivity system to be accessed only by the designated IT personnel, the intranet and the timekeeping systems to be accessed only by the managers, etc.
- To implement a prior authorisation procedure for the use of the employees' personal devices (BYOD).

**b) Technical measures**

- To offer the employees access only via a VPN type solution or any other security solutions ensuring similar security protection.
- To provide secured virtual solutions to ensure digital certification, such as use of electronic signatures, virtual approval workflows, etc.
- To ensure a periodically performing of a backup of all the important files.
- To implement appropriate IT solutions in order to counteract fraudulent actions of hackers attempting to take advantage of the remote work status, including by spreading ransomware and using phishing techniques having as a pretext COVID-19 news.
- To ensure that the IT infrastructure for the remote access has enough capacity and licenses to cover the increased number of users requiring simultaneous access, including by performing network load tests.
- To ensure that automatic updates of the employees' work computers also perform when they are working remotely.
- To remind the employees to update regularly the workstation, the security software and any other security tools, such as the add-ons for the browsers.

**2. What recommendations can the employers give to the staff that is working from home?**

- To use only the tools and communication channels made available by the organisation and remind the employees periodically that the security policies also apply when working from home (e.g. the rules for using private email accounts and file exchange services).
- To use, to the extent possible, the mobile phone 4G or 5G data network, as these ensure adequate security of the information from and to the device.
- To use only a secure Wi-Fi connection to prevent the interception and the access to the personal data to unauthorised persons.
- To ensure physical access to their work computer is secure, for example, by locking the screen when they are not working.
- To be cautious of any e-mails asking them to check or renew their credentials, to access various links or to send various information/ documents (as the case may

be), even if it seems to come from a trusted source. To encourage the employees to verify the authenticity of the request through any other means.

*ciprian.timofte@tuca.ro*

*florentina.petrisor@tuca.ro*

# Editors

**COVID-19 Legal Insights** is our response to the COVID-19 outbreak. We shall keep you informed on the various legal challenges posed by the coronavirus, thanks to a dedicated practice group comprising lawyers with different backgrounds, such as compliance/regulatory, corporate and commercial, insurance, labour and employment, litigation and arbitration, insolvency, public procurement, data privacy, tax and customs. In addition, our taskforce offers strategic advice on crisis-specific matters: corporate restructuring, review and (re)negotiation of agreements (including collective bargaining agreements and individual employment contracts), performance of the contracts which are affected by force majeure and hardship, unblocking pre-litigation relationships, etc. To keep abreast of developments, please feel free to regularly check our dedicated online resource: *http://www.tuca.ro/covid-19/*

Ciprian Timofte
Partner
+4 0374 136 341
ciprian.timofte@tuca.ro

TUCA ZBARCEA
ASOCIATII
Şos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, Bucureşti, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
*www.tuca.ro*