COVID-19: EUROPEAN BUSINESS CONTINUITY WHILE MITIGATING DATA PROTECTION AND SECURITY CHALLENGES FROM A DISTANCE

Date: 31 March 2020

EU Data Protection, Privacy, and Security Alert

By: Jeroen Smets, Claude-Étienne Armingaud, Patrice Corbiau, Natali Adison

With COVID-19 officially declared a pandemic by the World Health Organization, European governments and companies, facing unprecedented challenges, are encouraging their employees to work from home, protect their health and support government measures. Through these difficult times, it remains extremely important for European companies to take swift action, follow up on their projects on a daily basis and to ensure that data security and privacy protection measures are in place and are strictly monitored by professionals at all times. Privacy and data protection violations during COVID-19 times cannot be justified and may be investigated by the data protection authorities, whether it be during or after the crisis.
The current COVID-19 outbreak presents a significant challenge to cybersecurity in general, as ill-intentioned agents are seeking to capitalize through system disruptions and exploit employee confusions as the COVID-19 outbreak expands. Given the increase of COVID-19-related phishing emails, cybersecurity risks are expected to increase. Consequently, companies should adapt their information technology security requirements accordingly.

As companies may be struggling to adapt to this new reality, our key takeaways highlight important privacy, data protection and security challenges and provide practical advice for companies and professionals working from home, enabling them to ensure compliance in COVID-19 times.

TAKE A CLOSER LOOK AT HOMEWORKING IMPACTS

Before allowing professionals to work from home, companies should review their contracts, check up on their own and their professionals' tech equipment and do their due diligence. In particular, companies should at least double check the following:

- Can professionals be accommodated with the necessary tech equipment, enabling them to complete their tasks while working remotely?
- Do professionals have a suitable space at home from where they can work, as the case may be, safeguarding confidential and sensitive material?
- Can professionals easily and safely access the company's virtual workspace?
- Do the company's contractual relationships and obligations towards third parties allow working from home?

When answering these questions, companies may encounter certain privacy, data protection and security challenges. For example, some data protection agreements may contain corresponding and sharing prohibitions related to specific persons and or specific places. Consequently, violating these prohibitions could potentially lead to breach of contract or even to the termination of the contracts by the business partners. Moreover, in some cases, professionals will be obliged to work on their personal devices, which may lack the sufficient data and security protection settings, and/or may not have a suitable space to work from.

BE VIGILANT AND KEEP YOUR DATA PROTECTION FUNDAMENTALS UPDATED

The General Data Protection Regulation (GDPR) requires that companies comply with personal data protection requirements and that all necessary privacy, data protection and security documentation and procedures are in place whenever processing personal data. While personal data processing operations are either performed or overseen by a company's personnel, such company, as a “data controller” (or “data processor”), will remain directly liable for the damage caused by any breach of GDPR -- either from a regulatory point of view or a contractual one.

During the ongoing pandemic, where professionals are either encouraged or forced to work from home, companies must ensure they have proper policies in place to make sure their remote teams maintain the adequate security of all the company's data secure.

Such policies would notably to encompass:

- Data protection documentation, particularly any data protection impact assessment which may be required, as well as records of processing activities (RoPA), which need to be updated to encompass any specific processing implemented specifically for the COVID-19 pandemic (e.g. monitoring exposure, symptoms, absences);
- Ad hoc trainings to professionals regarding privacy, data and security compliance when working remotely, in particular, with regard to the requirements for collecting and sharing information (lawfulness, proportionality, transparency, minimization and retention);
- Reminders about maintaining the same levels of due diligence and confidentiality as applied inside the workspace while working remotely;
- Relevant safeguards for company-wide data transfers, including, as the case may be transfers outside the European Economic Area (whether or not related to COVID-19), to ensure the seamless and compliant sharing of personal data amongst their different group entities (e.g. Standard Contractual Clauses…);
- Assessment of the new processing operations which may be implemented specifically in relation with the COVID-19 pandemic, notably any health-related data which belong to the “special categories of data” subject to higher standards under GDPR, particularly of any restriction of access to implement, limitation of the data collected and shared, and necessity to collect such data with regard to the purposes considered; and

- Specific process in place to be able to handle data subject access requests, especially regarding COVID-19 concerns.

In addition, especially during times where face-to-face discussion may not occur, companies should keep their personnel updated in real time about potential privacy, data protection and security risks.

LIMIT CYBERSECURITY RISKS IN COVID-19 TIMES

Increasingly in times of crisis, professionals may be accessing (or transferring) company trade secrets, confidential information and/or (sensitive) personal data, via their personal devices. Such operations may increase the risks for data breaches and liabilities.

To limit such potential risks, companies should consider, for instance:

- Establishing data security guidelines, privacy and data protection policies and data retention guidelines, if not already in place, providing information about the potential personal data and security risks and consequences and how their impact can be minimized;
- Creating dedicated, secured and encrypted company email accounts and encouraging professionals to use them for all possible company-related communication purposes;
- Implementing mobile device management and mobile application management, which help manage and secure mobile devices and applications. The latter allow companies to remotely implement a number of security measures, including data encryption, malware scans, copy blocking and wiping data on stolen devices;
- Reminding their personnel of their duties to ensure the security of the company's confidential information, regardless of the place and/or device of access, and practical guidelines and examples, such as not leaving their devices unattended or unlocked;
- Reminding professionals, where available, to use a secured VPN network to access the company's information system and, where unavailable, to at least equip their devices with the company's security software;
- Reminding professionals to only use secure password-protected Wi-Fi and prohibit the use of public Wi-Fi;
- Reminding professionals, based on the company's guidelines, that company information should never be downloaded or saved onto personal devices or cloud services, including thumb drives, or cloud-based services;
- Training professionals on how to detect COVID-19-related phishing emails and handle phishing attacks and other forms of social engineering involving remote devices and remote access to company information systems;
- Protecting voice communications and enterprise telephony from unauthorized access and data theft by implementing cryptographically strong ID screening measures by default and remind professionals to log

in and out of every conference call meeting and not to remain constantly online, in order to avoid potential hijacking of the company's personal data, which could lead to data breaches;

- Assessing whether the company's cyber insurance coverage is adequate to cover the risks that may potentially be caused during the COVID-19 pandemic. Policy terms and conditions may need to be adapted in order to include and/or expressly deal with COVID-19 or other pandemics.
  Considering all of the above, now more than ever, it is important for companies to stay updated, available and have a data breach plan in place. This data breach plan should include a specific contact person who should be notified and procedure details to be followed in the unfortunate case where a data breach occurs.

If you would like to receive more information about potential data protection and security challenges when homeworking during the COVID-19 crisis, our K&L Gates Data Protection team remains available to assist you during these difficult times.

KEY CONTACTS

JEROEN SMETS
PARTNER

BRUSSELS
+32.2.336.1918
JEROEN.SMETS@KLGATES.COM

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

PATRICE CORBIAU
PARTNER

BRUSSELS
+32.2.336.1902
PATRICE.CORBIAU@KLGATES.COM

