April 2020

COVID-19 and Business Continuity in the EU

By David Dumont and Anna Pateraki

As the COVID-19 outbreak continues to unfold, businesses are dealing with new and unprecedented operational and legal challenges. This article discusses key data protection considerations for businesses in connection with the COVID-19 pandemic, including the processing of personal data for health-monitoring purposes, crisis management and cybersecurity preparedness, and steps businesses may take to ensure the business continuity of privacy compliance programs.

I. PROCESSING OF PERSONAL DATA FOR COVID-19 DETECTION AND PREVENTION PURPOSES

Over the past weeks, data protection authorities in the EU and the European Data Protection Board (EDPB) have issued guidance on the processing of personal data, including health data, for COVID-19 detection and prevention purposes. The general message of the authorities has been consistent: the EU General Data Protection Regulation (GDPR) does not prevent the processing and disclosure of personal data that is necessary to fight the COVID-19 pandemic.

Nonetheless, it is important that the general data protection principles set forth by the GDPR are respected, even during a crisis. In terms of lawfulness, several legal bases of the GDPR can be relied upon to legitimize the processing of personal data for COVID-19 detection and prevention purposes, including the legitimate interests legal basis. In addition, for the processing of health data, which is considered sensitive personal data under the GDPR, EU data protection authorities have identified various legal bases on which companies may be able to rely. For example, companies may be able to assert that the processing of health data of employees is necessary for companies to carry out their obligation under local labor law to ensure health and safety in the workplace or for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.

All data processing operations, however, must be proportionate to the purpose that the data controller is seeking to achieve. In addition, the data processing must respect the other data protection principles and requirements set forth by the GDPR, such as the principle of data minimization (i.e., avoiding excessive information collection) and the requirement for transparency (i.e., ensuring that data subjects are fully aware of the processing of their personal data for COVID-19 detection and prevention purposes).

EU data protection authorities, among others, have issued recommendations for a number of practices involving the processing of personal data for COVID-19 detection and prevention purposes, including:

- **Surveys, tests and reporting:** As a general best practice, companies should avoid conducting systematic surveys for COVID-19 infections of employees or their relatives, contractors and visitors. Conducting mandatory temperature tests of these individuals similarly may be problematic from a proportionality perspective, but mandatory temperature tests could be justified in limited individual cases if no other less intrusive measures are available. With respect to reporting, companies may encourage employees, contractors and visitors to voluntarily report travel to any high-risk areas, but companies should avoid issuing mandatory questionnaires regarding all recent travel.
- **Identity of infected employees:** Due to confidentiality and data minimization obligations, companies generally should not reveal the names of employees infected with COVID-19, but may inform others (including coworkers, customers and public authorities) about an infection or the number of infections within the company's workforce. If revealing the name of an employee who contracted the virus is strictly necessary for prevention purposes and the applicable national law permits doing so, the employee at issue should receive advance notice.
- **Employees' personal contact details:** In general, the processing of employees' personal contact details, such as private cell phone number and email address, is allowed to the extent necessary for the employer to communicate with the relevant employee for COVID-19 detection and prevention purposes.

Although there is a certain level of consistency in the COVID-19-related issues addressed by regulators, guidance of EU data protection authorities around these issues varies by country. As a result, when designing COVID-19 detection and prevention measures involving the processing of personal data, companies operating in multiple EU Member States should examine requirements and regulatory guidance at a national level.

II. CRISIS MANAGEMENT

A. Cybersecurity Preparedness

The number of cyberattacks to company systems have increased and likely will continue to increase as a result of businesses' and workforces' moving online in response to COVID-19 confinement measures. Cyberattacks can cause disruption to company systems and expose personal data to unauthorized access by third parties. In light of these concerns, it is important to review and, if necessary, revise the company's cybersecurity preparedness measures and incident response plans to ensure that they are adapted to the new reality of doing business remotely. This can include, for example, the following measures:

- **Incident response readiness:** Intensifying the routine exercise of information security teams, such as those who monitor access logs to detect suspicious behavior, investigate alerts, perform security audits and controls, detect and mitigate security threats and vulnerabilities, and immediately report issues to the company's leadership. In addition, because there could be

challenges associated with tasks that require physical presence, incident response teams should consider identifying such tasks and developing solutions for preparedness purposes.

- **Data loss prevention:** Improving encryption and rolling out tools and guidelines that will help prevent data loss while employees continue to work remotely, especially if employees use personal devices to perform professional tasks. It also is important to ensure that all company-owned devices used by employees to perform their job remotely have state-of-the-art encryption, as this factor may be considered when addressing potential breach notification obligations of the company in the event a device gets lost or stolen.
- **Phishing:** Reminding company employees to consult only trusted sources and avoid clicking on links or opening attachments in unsolicited emails. The number of COVID-19 phishing email attempts that could expose corporate networks to hackers and other malicious activity have been increasing.
- **Authentication:** Reviewing the security of the company's authentication interfaces and enhancing multifactor authentication techniques for logging on to the company's network, where required, to limit intrusion risk.
- **Contact details:** Ensuring that employees who telework know who to contact within the organization to report a security incident or personal data breach.

B. Safe Teleworking

As businesses continue to rely heavily on teleworking, companies also should consider setting up, or finalizing the setup of, employee remote working practices to ensure the safety of company systems, including the protection of personal data residing on those systems. For example, allowing employees to use personal devices to connect to the company's network may pose particular risks for system security and unauthorized disclosure of personal data. These risks typically should be addressed in a robust bring-your-own-device (BYOD) policy. Companies also should consider providing appropriate training to educate employees and raise awareness about safe teleworking issues, such as which cloud-based resources employees may use when working remotely, using a secure internet connection, the importance of using strong passwords, implementing firewalls and anti-virus protection on any personal devices, and securely transmitting or disposing of documents containing personal data. As a best practice, companies should establish guidelines regarding handling files at home where required, such as for HR managers who may need to transfer employee files to their home office during the teleworking period.

To the extent that the teleworking situation is likely to last for a long period or become the company's standard, the company should consider developing and maintaining a safe teleworking policy. Alternatively, updates to relevant parts of existing policies, such as an IT system's monitoring policy or acceptable use policy, could achieve the same result.

A practical way to raise awareness internally about safe teleworking is to provide examples in the relevant policy or communication regarding unsafe behavior that puts information security and personal data at risk when employees work from home (e.g., changing laptop settings, letting others at home use the company device for personal use, sending confidential documents to personal email accounts or allowing others to overhear business conversations). Updates to other company policies also may be

required because of the novel teleworking situation and the particular risks related to teleworking, such as information security policies. Directing employees to the relevant resources and issuing updates or reminders in stages, to manage priorities effectively, would be useful. Teleworking also may raise new challenges for existing employee monitoring practices or create a need for additional employee monitoring measures, which should be assessed from a national labor and data protection law perspective.

C. Vendor Management

As the implications of COVID-19 continue to evolve, identifying the vendors that are critical to the company's business, services or communications (e.g., video conference vendors) is recommended for business continuity purposes. For key vendors, companies should consider (i) listing the relevant contact persons and their respective contact details and (ii) identifying alternative resources that may be used if necessary to mitigate an immediate data protection issue involving the vendor.

Vendor data protection issues may vary depending on the vendor's type of business, but such issues could include, for example, (i) disruptions in individuals' availability and workflow continuity due to the unavailability or technical inability of the vendor to provide a service or fix an issue, (ii) data security issues, (iii) issues deleting personal data after the termination of the service or (iv) a delay in notifying customers in the event of a data breach. In anticipation of potential issues, contracts or relationships with key vendors may need to be reviewed to strengthen protections such as data security and incident notification or to identify alternative contacts in case certain contact persons become unavailable.

III. ORGANIZATIONAL MEASURES FOR BUSINESS CONTINUITY

In times of uncertainty, ensuring the ongoing availability of resources within an organization is important to limit disruption to daily business operations and maintain appropriate internal governance.

- **Leadership and oversight:** To handle a crisis effectively, it is important that senior leadership and their support functions remain available and continue their oversight when working remotely. These essential parties and functions can include the general counsel office, the chief privacy officer's team, the data protection officer's team, the incident response team, and procurement and vendor management functions. In addition, employees should know who to contact for data protection review of products and services in the event key individuals or the data protection officer becomes unavailable. Organizations should consider maintaining an inventory of leadership and senior management with data protection responsibilities, relevant review teams, their current contact details, availabilities, replacements and media where key business information and correspondence is stored, in case someone becomes temporarily unavailable. This will help with obtaining approvals, issuing notifications and making decisions regarding the processing of personal data in connection with product updates or employee privacy issues as business operations continue amidst the pandemic.
- **Accountability and escalation process:** While personnel are settling in their home offices and business meetings are held remotely, documentation required to demonstrate a company's accountability with respect to the processing of personal data should not fall through the cracks. For example, knowing how and by whom data protection impact assessments (DPIAs) will

continue to be conducted and having in place a process for maintaining records of current data processing activities are both vital. Taking these steps also will help relevant teams know how high-risk privacy matters should be escalated internally if required for making decisions during an emergency event.

- **Data Subject Requests:** Companies likely will continue to receive requests from data subjects exercising their data protection rights under the GDPR, such as their rights of access to or deletion of their personal data. From an operational perspective, it would be helpful to consider how the company will handle data subject rights requests moving forward. The GDPR requires companies to assess and respond to such requests within one month of receiving the request, but it permits an extension by two further months where necessary, taking into account the complexity and number of requests. If an extension is required, the company should communicate to the data subject the reason for requesting the extension and document the reasons the company is unable to meet the statutory timelines. At this time, data protection authorities generally seem to understand that the challenges companies currently are facing in trying to handle business operations during the COVID-19 outbreak may require diverting resources to prioritize other areas. Although some data protection authorities (e.g., UK, Ireland) have issued statements in support of the understandable delays individuals may experience when dealing with organizations that are at the frontline of fighting the pandemic (for example, health care providers and government departments), the authorities are not able to extend statutory timescales. As a result, companies facing issues in responding to data subject requests should consider implementing a pragmatic plan based on available resources to provide information in phases where possible and to request an extension, where necessary and appropriate.

David Dumont is a partner in Hunton Andrews Kurth's Brussels office. He can be reached at DDumont@huntonAK.com. Anna Pateraki is a senior associate in the firm's Brussels office, and she can be reached at APateraki@huntonAK.com.