McKinsey & Company

Risk Practice

Privacy, security, and public health in a pandemic year

How can European companies best prevent measures intended to control the COVID-19 pandemic from also undermining data privacy and security?

by Daniel Mikkelsen, Henning Soller, and Malin Strandell-Jansson

June 2020

As the coronavirus pandemic takes its terrible toll, in both human life and livelihoods, governments, public-health authorities, companies, and individuals have responded with extraordinary measures. To protect the health of people, governments and institutions put in place restrictions on movement and mechanisms for health tracking and reporting. These mechanisms, including contact-tracing and self-reporting apps, some recording and transmitting personal health information, underscore the deepening importance of data protection and privacy in this crisis.

With the advent of the European General Data Protection Regulation (GDPR) in 2018 and the possible "ePrivacy Regulation," companies and institutions have increased their data awareness. These new regulations enforce stricter rules on privacy and data protection, setting new standards, in the words of the GDPR, for the "rights and freedoms of data subjects" around the globe. During the pandemic, government authorities and companies have had to balance two priorities—protecting public health and protecting personal privacy. Some measures designed to limit the spread of the virus and potentially save lives could also have serious human-rights implications.

While many public-health measures do not require data collection, others could encroach upon the protections that protect individuals' personal data. Government officials and companies can find themselves on the horns of a dilemma, so to speak, contemplating measures to reduce the spread of the virus that could meanwhile drastically curtail the rights and freedoms of the people whose lives they seek to protect. The following discussion draws on the recent European experience of this public health–personal privacy dilemma. Events continue to move quickly, and our analysis reflects experience at a particular point in time (May 2020) in the history of the pandemic.

Pandemic controls and personal freedom

The primary focus for public authorities and the private sector is to control the disease. The protection of human life is the all-important foundation for any further steps taken to return to normalcy. To this end, healthcare systems, including personnel, facilities, tests, and necessary equipment (including ventilators and personal protective equipment or PPE) must be secured and expanded as needed. State budgets have been vastly expanded to address extraordinary demands. The measures introduced to limit the reach of the virus have affected personal freedom in three basic areas:

— *Limits on personal movement,* including physical distancing, restrictions on public gatherings, quarantine, isolation, and lockdown.

— *Health reporting,* including COVID-19 testing, temperature testing, public- and private-sector health surveys, public-authority and corporate-internal reporting.

— *Health-tracking,* including manual and automated tracking and contact-tracing mechanisms (mobile-phone tracking and applications), by both states and private companies.

Many of the protective measures governments are taking in these areas are well understood and supported by the affected populations. Concerns are being raised, however, about their intrusiveness on personal privacy and implications for the future. Government officials and corporate-privacy officers struggle with balancing protection measures and privacy safeguards, often without clear guidance from regulators. In the private sector, corporate boards and top management have tended not to prioritize privacy aspects in the fight against the virus.

Beyond the risks posed in the handling and processing of personal data, systemic cyberrisks are posed in the COVID-19 working environment. With workplaces closed and employees working from home, the IT departments of public institutions and companies have had to set up remote operations rapidly. Many people are now using unsecured devices and internet communications with lower protection levels than those maintained in corporate or institutional networks. The performance of network infrastructure being deployed is potentially weaker and less subject to human control and support from other employees. Increased system stress and gaps in collaborative tools have led to increased vulnerability, as witnessed in numerous reports of higher levels of cyberattacks, including malware-laced email phishing, scammers posing as corporate help desks, and malware in COVID-19 information sites. The threats are all designed to take advantage of remote working arrangements in place since the beginning of the pandemic lockdowns.

The GDPR under stressed conditions

Like public and private organizations, regulators too were unprepared for the COVID-19 crisis. After a period of adjustment, however, they are now providing guidance and clarification on how to interpret existing legislation in the crisis environment, with particular attention to health-related protective measures introduced or being considered by companies.

The GDPR is considered by experts to be one of the world's strictest privacy regulations. The consensus among European regulators and the European data protection supervisor is that the current crisis does not nullify the GDPR, but that its rules are flexible enough to accommodate the emergency measures while keeping in place adequate safeguards. According to the GDPR, for example, national governments are permitted to act in the public interest, but must limit the data they use.

A few principles advanced in the GDPR are important in this respect. The regulation requires "data minimization" and "purpose limitation." These two guidelines specify that as little personal data as necessary should be used and for a specific, narrow purpose only—in this case, to limit the spread of the virus and protect employees' health. Transparency is also required, meaning that affected individuals must be informed about the usage of their data in simple, clear language. A further principle is protection: data must be sufficiently protected both technically against cyberrisk and organizationally against unauthorized sharing.

Like public and private organizations, regulators too were unprepared for the COVID-19 crisis.

To help companies understand the data-protection rules, many European regulators have issued guidance on specific health measures. This guidance mostly addresses situations for which consent is not a practical consideration, such as notifying the specific employees who have worked in close proximity to an infected person. The guidance also varies slightly from country to country, depending on national legislation related to health, labor, and social security, and their varying interpretations. We have identified common guardrails around the three types of control measures listed above. The following considerations are, however, subject to further assessment on a case-by-case basis, according to national laws and pertinent legal guidance. (The discussions in this article are not intended to give such legal guidance.)

Limits on personal movement

The limits on personal movement imposed by public authorities in the crisis are not usually addressed in data-protection laws. Such limits are intrusive of people's rights and freedoms, however, and may even be subject to other laws. Employer mandates for working from home likewise fall outside data-protection laws, as has been emphasized by several European data-protection authorities.

Entrance controls at places of employment can, however, present data-protection issues. In the view of many regulators, employees returning to work could be required to disclose travel information in connection with public-health concerns. If they have been to a high-risk area, appropriate action (such as temporary quarantining) can be mandated. Regulators have expressed concern over temperature taking and personal health surveys. Both Swedish and Belgian data-protection authorities, for example, do not consider the measurement of body temperature to fall under the GDPR, unless the results are recorded. But other regulators have specifically forbidden regular temperature taking.

Health reporting

According to the GDPR and other European regulations, employers are generally not permitted to collect health data from employees and visitors, except when legally obligated to do so, whether to protect the interests of the workforce or the public, or to comply with employment law or other national laws. Where the exceptions apply, data processing must be strictly limited, according to the principles of data minimization, purpose limitation, transparency, and data protection. Employers are only permitted to collect as few data as necessary for a specific purpose. They must inform the individuals concerned about data processing and ensure that the data are appropriately protected. The processing must be documented and it must also be stopped as soon as it is no longer needed.

Employers are not permitted generally to provide employees with the names of colleagues who have fallen ill, apart from notifying a narrow list of those with whom they have had close contact. The GDPR also limits the right to ask for employees' private phone numbers except for specific reasons, such as to inform individuals of work rules and other information relating to the COVID-19 pandemic. In accordance with GDPR principles, furthermore, usage of data of vulnerable individuals in higher-risk groups should be limited to specific purposes (such as home deliveries of vital supplies).

Health tracking

The GDPR puts certain privacy and data protections in place that limit the possible health-tracking measures, which countries may use in the COVID-19 crisis. European data-protection authorities have, however, permitted deployment of national tracking systems as long as they are aligned with GDPR principles. The systems must be voluntary and consensual or fully anonymized, as when a telecommunications operator supplies authorities with anonymous data for measuring population movement. More precise personal monitoring

systems, such as those utilized in South Korea or China to contain the spread of the pandemic, are not permitted under the GDPR.

Cybersecurity considerations

In the pandemic, IT departments have faced completely new challenges, as entire workforces were sent home to work remotely. Companies must now maintain the security of their systems, software, and data outside the centralized, well-controlled corporate network, while also meeting GDPR requirements on appropriate technical and organizational cyber protections. Employees are using individual links to connect to networks, while IT departments struggle with rapid and unplanned scaling-up of infrastructure. New and untested features, along with suboptimal controls, are being used to ensure business operations.

An understanding of the cyberrisks inherent in the new network arrangements is still emerging. Suspicious cyber domains purportedly relating to COVID-19, selling fake cures or circulating malware, have proliferated at an alarming rate.[1] Government entities and companies are now developing protective measures against these threats, involving new tools, awareness, and training.

Companies are providing employees with laptops, mobile phones, and other necessary equipment to secure virtual-private-network (VPN) connections so that they may work remotely. Employers must also provide employees with an array of other technical features to secure their networks. This includes patch and configuration management for relevant systems, multifactor identification and secure-access management, on-premise application security for remote access, device virtualization, capacity and security monitoring, and contingency resources (to limit the effects of failures and breakdowns).

Employees need to be informed of the special technical features enabling secure remote operations and trained as needed in their use. The importance of security in working remotely needs to be stressed, and the VPN made mandatory. Employers also must provide guidelines on a host of related topics, restricting the use of private devices, recommending particular software applications, supplying adequate password protection, as well as formulating instructions for protecting hardware and hard copies of documents.

Employees should also be educated about the rising level of coronavirus-related cyberthreats, including potential responses and incident handling. Employers should be working to ensure that risk-averse behavior becomes the norm in these extra-normal times. Experience has shown that messages on data protection and compliance are best transmitted in ongoing communication efforts rather than in time-limited campaigns.

In general, employers are responsible for providing an adequate support environment, including training in potential security risks and the secure use of the new remote tools. Ready access to support channels should also be provided as needed. Employees without an adequate technical setup at home will have to be provided with one; those unused to working from home or communicating through video applications may need some basic guidance. Everyone will have to be made aware of what should happen in case of a breach, including reporting lines to use and actions to be taken.

The crisis has thus increased workloads on IT and cybersecurity departments. Companies may need to address capacity constraints in these areas and also introduce measures to safeguard the well-being of employees. One way to do this is to add specialists where needed or for specific high-demand periods. By reducing demand to

[1] Daphne Leprince-Ringuet, "Domain name registry suspends 600 suspicious coronavirus websites," ZDNet, April 7, 2020, zdnet.com.

sustainable levels, IT and cyber staffers will breath easier and be better able to protect the organization and its technology.

Most if not all regulators are aware of the strains that the COVID-19 crisis is putting on organizations. In recognition, some are introducing flexibility around privacy-related processes and timelines. For example, the Information Commissioner's Office (ICO), Britain's data-protection authority, has announced that they will not strictly enforce deadlines for data-subject-rights requests. The Dutch authority, Autoriteit Persoonsgegevens, has stated that pending issues will be granted longer response periods. In Ireland, the Data Protection Commission, expressing awareness of the situation, has stated that requests for leeway in meeting deadlines will be evaluated on a case-by-case basis.

Three productive actions

Companies are making a number of adjustments to ensure a balanced approach to data privacy and health protection in the COVID-19 context. In our view, three actions will be most productive of deliberate decision making on data privacy and cybersecurity during the COVID-19 dislocations.

- Include a data-privacy leader in the organization's COVID-19 response team to ensure early evaluation and discussion of possible measures affecting data privacy. This leader (likely the data-privacy officer, for those organizations that have one) should also be charged with making any necessary trade-offs between privacy and public-health needs, designing regional variations as required.

- Provide IT departments with the resources needed to support employees working securely from home. Likely companies will have to expand their network and videoconferencing capacity with vendor-supplied services. These should match internal security standards without exceeding bandwidth limitations.

- Establish dedicated support and training in risks and mitigating measures for remote working, including clear ongoing communications. This work should include focused efforts with appropriate vendors to find possible security gaps and to develop solutions for closing them.

Taking these actions will help enable clear direction and guidance on health and privacy measures, and go a long way to stabilizing operations for the duration.

Daniel Mikkelsen is a senior partner in McKinsey's London office, **Henning Soller** is a partner in the Frankfurt office, and **Malin Strandell-Jansson** is a senior knowledge expert in the Stockholm office.

Designed by Global Editorial Services