GIBSON DUNN

Privacy and Cybersecurity Issues Related to COVID-19

Client Alert | March 20, 2020

Whatever industry you are in, you are undoubtedly concerned about the threat of the novel coronavirus (COVID-19).[1] Below, we summarize key privacy and cybersecurity implications of collecting and sharing personal information from employees, site visitors, and other individuals to manage COVID-19 risk, as well as cybersecurity risks of these and other management and mitigation efforts.

Despite the need to take swift action in this rapidly evolving environment, we recommend that companies consider how to do so in a manner that minimizes privacy- and cybersecurity-related legal risks. Various regulatory agencies have issued guidance in the last several days indicating that privacy laws that limit the collection and disclosure of personal information remain in effect. And the implementation of work-from-home and other arrangements has increased exposure to various cybersecurity risks—risks that hackers have moved swiftly to exploit.

The United States

Though there is no federal data protection law in the United States, the Centers for Disease Control and Prevention ("CDC") and the US Equal Employment Opportunity Commission ("EEOC") have advised employers to keep certain personal health data confidential, and most companies have made commitments to their employees, customers, and/or users about keeping their personal health data confidential. In addition, some state laws, such as the California Consumer Privacy Act ("CCPA"), impose transparency requirements on covered businesses, and may result in additional liabilities in light of data breaches.

Generally, when implementing COVID-19 risk mitigation measures in the United States, companies may wish to consider the following privacy and cybersecurity-focused steps:

- ***Provide notice before collecting and limit use of personal information***. If you decide to collect additional personal information at this time, particularly sensitive personal data, such as health or medical information, whether through the use of surveillance technologies such as thermal cameras or otherwise, consider notifying employees, visitors, or any individuals prior to such collection. For example, the CCPA requires that covered businesses provide notice to California residents (including employees) regarding the categories of information collected and uses of that information at or before the time of collection; even where companies and employers have implemented CCPA-compliant privacy policies, the collections and uses of personal information for the COVID-19 pandemic may be sufficiently novel that additional notice is required.[2] Companies should, however, be cautious about the language employed to notify individuals of these data collection practices, especially being careful not to concede that the company is *processing* the data, if accurate (for example, information reviewed for real-time monitoring may be treated differently by regulatory authorities than health information the company chooses to store for potential further use).For companies collecting additional information, including sensitive health or medical data, consider limiting

Related People

Ryan T. Bergsieker

Cassandra L. Gaedt-Sheckter

Ahmed Baladi

Patrick Doris

Vera Lukic

Kai Gesing

Clémence Pugnet

the company's use and retention of such data to the monitoring of health and public safety conditions at work, and de-identify the data to the extent possible. Before considering any further uses or retention of such data, consider contacting outside counsel to properly weigh potential privacy risks.

- ***Implement reasonable security protocols and issue cybersecurity reminders to employees***. Consider implementing reasonable security protocols and data minimization efforts that are appropriate to the sensitivity of the personal information, such as encryption, data separation, and data access controls, to collect and store data. For instance, the Genetic Information Nondiscrimination Act ("GINA")[3] requires that information obtained pursuant to medical examinations of employees must be collected and maintained on separate systems and treated confidentially.[4] And the CCPA threatens a private right of action and/or enforcement if businesses suffer a data breach due to its "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[5] Consider also limiting collection, use, and retention of such data to what is absolutely necessary.Additionally, cybersecurity threat actors are particularly likely to exploit vulnerabilities in companies' IT systems to gain access to sensitive personal information during these times of turmoil, particularly as companies are struggling to implement unprecedented work-from-home policies and information is less centralized. Cybersecurity firms have reported an increase in malware attacks in which threat actors have used the widespread panic related to COVID-19 to trick victims into running malware.[6] Hackers are actively targeting companies that launched a work-from-home policy in response to the COVID-19 outbreak by exploiting outdated virtual private networks, a lack of multi-factor authentication, and insecure at-home servers.[7] In light of this potential increase in the exploitation of cybersecurity vulnerabilities, consider re-evaluating your cyber-security posture and issuing reminders to employees to be on the lookout for phishing attempts, to employ secure connections, and that the company will not collect passwords or personal information relating to their online accounts, as part of the company's coordinated COVID-19 response efforts. Indeed, in discussing the CCPA during the COVID-19 crisis, an advisor to the California Attorney General has been quoted as "encourag[ing] businesses to be particularly mindful of data security in this time of emergency."[8]
- ***Seek counsel before implementing any preventative or reactive data collecting or sharing measures.*** Details and circumstances related to COVID-19 are changing constantly and the impulse to collect and share data to help stop its spread can be strong. Privacy rules and requirements, however, must also be kept in mind and considered, particularly in light of potential additional liabilities under new laws, such as the CCPA.

In the event that you learn that an employee or visitor to your facilities tests positive for COVID-19, consider taking the following steps to lessen the company's exposure to privacy-related liability:

- ***Consider how you learn about an employee's exposure.*** Companies should consider having prepared responses ready for communications with affected employees. Whether the company learns directly from the affected employee or indirectly, the prepared response may notify the employee that their exposure to COVID-19 will be communicated to other employees, but that their identity will not be revealed. If the company learns directly from the employee, the company's response may also convey appreciation for the employee's willingness to come forward.
- ***Inform potentially exposed employees without disclosing the identity of affected individuals***. Consistent with the advice above, the CDC has advised employers to inform fellow employees of their possible exposure to COVID-19, but warned against disclosing the identity of the individual who tested positive.[9] Companies may also wish to advise potentially impacted customers, vendors, and visitors of their exposure, while maintaining the confidentiality of the affected

individual.

- ***Maintain confidentiality and promises made in Employee Handbooks and Terms of Use***. A number of federal laws, including the Americans with Disabilities Act ("ADA"),[10] and GINA,[11] and regulations promulgated pursuant to the Family and Medical Leave Act of 1993 ("FMLA"),[12] impose confidentiality requirements related to medical and health data of employees. In general, the EEOC has advised that "[e]mployers must maintain all information about employee illness as a confidential medical record in compliance with the ADA."[13] Furthermore, employers should avoid involuntary disclosure of confidential information to employees' supervisors, although employers may share information about the specific accommodations needed by employees.[14]

Companies should also check their Employee Handbooks and Terms of Use to ensure that any promises made in those documents are carried out—or updated with clear notice to employees—before implementing data collection and sharing practices. These promises should be acknowledged in any communications with employees, visitors, vendors, customers, or others, where applicable.

Europe

On March 19, 2020, the European Data Protection Board ("EDPB") adopted a statement on the processing of personal data in the context of COVID-19.[15] The statement emphasized that while data protection rules, including the European Union's General Data Protection Regulation ("GDPR") should not "hinder measures taken in the fight" against COVID-19, data controllers and processors must ensure, "even in these exceptional times," the protection of individuals' personal data. Specifically, the EDPB explained that any measure taken in this context should comply with general principles of law, adding that "emergency is a legal condition which may legitimize restrictions to freedom provided these restrictions are proportionate and limited to the emergency period."

Among the core data privacy principles to be abided, the EDPB highlighted that individuals should receive transparent information on processing activities, including related purposes for processing and retention periods. Companies must adopt adequate security measures and confidentiality policies, as well as document measures implemented and underlying decision-making processes to manage the current emergency.

With respect to legal bases for processing personal data, the EDPB explained that the GDPR provides legal grounds to enable employers and competent public health authorities to process data in the context of an epidemic, in accordance with national law and within the conditions set therein. In the employment context, the processing may be necessary "for compliance with a [national] legal obligation to which the employer is subject (such as obligations relating to health and safety at the workplace) or in the public interest, such as the control of diseases and other threats to health."[16] The EDPB also emphasized that the exceptions to the prohibition of processing of health data[17] may be available to companies "where it is necessary for reasons of substantial public interest in the area of public health"[18] or "where there is a need to protect the vital interests of the individual."[19] However, though the EDPB provided answers to some questions about the processing of data in the employment context, it failed to offer any concrete recommendations and limited its answers primarily to restating the general data protection rules (such as proportionality and data minimization principles) and relevant national laws.

Member State Data Protection Authorities ("DPAs") have also issued their own guidance in recent weeks with respect to the processing of personal data in this context.[20] These authorities have emphasized the general principles of lawfulness, necessity, transparency, and proportionality of the processing, as well as the principle of data minimization, set forth under the GDPR, and some have encouraged data controllers to refer to instructions and preventative measures issued by public health authorities for guidance. However, these

DPAs have generally failed to adopt a unified approach.

This legal context makes it challenging for companies to ensure compliance with applicable data privacy laws throughout Europe, let alone maintain consistency with a global approach, including the United States. Companies should consider carefully, in consultation with their legal department and outside counsel, the privacy implications in each European country of engaging in data collection and sharing in the context of the COVID-19 pandemic.

The following table summarizes the developments across Europe of several key DPAs with respect to the collection and processing of personal information in the context of the COVID-19 outbreak, with further detail following.

Data Protection Authority	Processing Legal Basis and Exceptions	Emergency Data Collection Measures	Application of Data Privacy Principles and Protections
Belgium	• Broad application of Art. 6(1)(d) not justified for prevention measures. • Companies cannot rely on Art. 9(2)(i) except upon express mandatory instructions from health authorities.	• Health risk assessment may only be carried out by the workplace doctor based on Art. 6(1)(c) and 9(2)(d).	• GDPR Principles are still applicable.
France	• Not addressed by DPA.	• Companies cannot implement mandatory and systematic body temperature measurement. • Employers may invite employees to report their potential exposure to COVID-19. • In the event of such employee's reporting, employers can record the identity of affected individuals and resulting remedial measures taken, and can	• GDPR Principles are still applicable.

		report elements related to the nature of the exposure to health authorities, on request.	
Germany	• Art. 9(2)(b) and 6(1) constitute relevant legal bases and exceptions to process health and other personal data.	• Employers can ask employees /visitors for appropriate health and other personal information for the purpose of reducing the spread of COVID-19.	• GDPR Principles are still applicable.
Spain	• Art. 9(2)(b) might constitute relevant legal basis and exception to process health and other personal data.	• Under Spanish labor and risk prevention laws, employers have a duty to protect employees from and prevent work risks, in consultation with Works Council.	• GDPR Principles are still applicable.
United Kingdom	• Not addressed by DPA.	• DPA considers asking people if they have visited a particular country or are experiencing COVID-19 symptoms to be reasonable. • On the collection of employee and visitor health data by companies, DPA stressed the general data protection principles.	• DPA will not penalize companies that might not meet usual privacy standards or deadlines to respond to data subject requests to the extent they need to prioritize other areas or adapt their usual approach during this period. • GDPR Principles are still applicable. • Statutory timescales are not to be extended, but

DPA will inform data subjects that they may experience delays when making information rights requests during the pandemic.

As the table reflects, the approach taken by European DPAs has varied significantly by jurisdiction:

- ***Belgium***

On March 13, 2020, the Belgian DPA stated that companies should not adopt a broad application of the legal basis that allows for processing necessary to safeguard the vital interests of the individuals under Article 6(1)(c) of the GDPR[21] when implementing preventive measures.[22] The Belgian authority also explicitly noted that companies cannot rely on Article 9(2)(b), which allows for the processing of personal data when it is "necessary for reasons of public interest in the area of public health," unless they are required to do so pursuant to explicit instructions from the Belgian health authorities. Rather, companies should rely on workplace doctors to inform employers and persons who have been in contact with the affected employee, in accordance with Articles 6(1)(c) and 9(2)(b) of the GDPR.

- ***France***

On March 6, 2020, the French DPA published guidance on the collection of data, and in particular employee data, in the context of COVID-19.[23] While the French authority provided that companies should refrain from implementing a mandatory body temperature measurement for employees/agents/visitors (similar to the position taken by the Belgian, Hungarian, and Luxembourgian DPAs), it indicated that employers may invite their employees to report their potential exposure to them or to the competent health authorities. In the event of such reporting, the employer is then entitled to record the date, identity of the allegedly affected individual, and the remedial measures taken (e.g., containment, remote working, contact with occupational health care resources), and to communicate information related to the nature of the exposure to health authorities, on request.

- ***Germany***

On March 13, 2020, and March 17, 2020, the German Conference of Federal and State Data Protection Authorities ("DSK") and several state-level DPAs published COVID-19 guidance on the collection and processing of health data, respectively.[24] The guidance confirms that Articles 9(2)(b) and 6(1) may provide the appropriate legal bases for the processing of relevant health data and other personal data in the context of the COVID-19 pandemic. Though this guidance suggests that a company may ask both employees and visitors for health-related information relevant to reduce risks to other employees and the public, it also emphasized that companies must process this information in accordance with general GDPR principles. Permissible questions would likely include asking whether individuals have tested positive for COVID-19, have been in contact with someone who has, or have recently visited an area classified as a risk area by the German Center for Disease Control, the Robert Koch Institute. Companies will likely also be permitted to collect and process information about employees who test positive for the virus or who have been exposed to affected individuals for the purposes of informing co-workers on an anonymous basis. While doctors and other medical personnel are required by law to report COVID-19 cases, this does not seem to apply to employers. However, the guidance is

ambiguous with respect to other data collection and processing practices, such as temperature testing.

- ***Spain***

On March 12, 2020, the Spanish DPA published a report regarding the processing of personal data in the context of the COVID-19 outbreak. Although the report is mainly applicable to the public administration, the authority stated that, in the context of employer-employee relationships, Articles 6(1)(c) and 9(2)(b) of the GDPR may constitute relevant legal bases and exceptions to process health and other personal data. Under Spanish labor and risk prevention laws, employers, in consultation with workers through Works Councils, have a duty to protect employees from and to prevent work risks, and to regularly monitor the health conditions of employees with respect to risks inherent to work, all the while respecting the right to privacy of employees and the confidentiality of the data.[25]

- ***United Kingdom***

On March 12, 2020, the United Kingdom DPA issued guidance that stated that it would not penalize companies that the DPA "knows need to prioritise other areas or adapt their usual approach during this extraordinary period."[26] It described itself as a "reasonable and pragmatic regulator, one that does not operate in isolation from matters of serious public concern."[27] The DPA stated: "Regarding compliance with data protection, we will take into account the compelling public interest in the current health emergency."[28] Conversely, in its discussion of the collection of health data of employees and visitors, the UK authority only emphasized the GDPR principles.

The UK DPA did note, however, that it was permissible to inform staff if a colleague contracted COVID-19, noting that the affected individual should not be named and no more information than is necessary should be shared. The UK authority also noted that it would be reasonable to ask employees if they had visited a particular country, or are experiencing COVID-19 symptoms.[29]

We will continue to monitor privacy and cybersecurity developments related to COVID-19 in the United States, Europe, and around the world, and will provide further communications as developments warrant.

---

[1] The lawyers on Gibson Dunn's cross-functional COVID-19 Response Team—who are linked with subject-matter experts throughout the firm—are available to assist with any questions you may have regarding developments related to the COVID-19 outbreak. *See* https://www.gibsondunn.com/coronavirus-covid-19-resource-center/.

[2] Though California Attorney General Xavier Becerra cannot bring enforcement actions until July 1, 2020, the California Chamber of Commerce, the Internet Coalition, the Association of National Advertisers and approximately 30 other companies across a range of industries sent the California Attorney General a letter calling for this impending deadline to be delayed until January 2, 2021 in order to allow companies more time to respond to the unique challenges posed by the COVID-19 outbreak. See Allison Grande, COVID-19 Warrants CCPA Enforcement Delay, Calif. AG Told, Law360 (March 19, 2020), available at https://www.law360.com/articles/1255181/covid-19-warrants-ccpa-enforcement-delay-calif-ag-told.

[3] Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 & 42 U.S.C.).

[4] 42 U.S.C. § 12112(d)(3).

[5] Cal. Civ. Code § 1798.150.

[6] Zack Whittaker, Hackers are jumping on the COVID-19 pandemic to spread malware, TechCrunch (March 12, 2020), available at https://techcrunch.com/2020/03/12/hackers-coronavirus-malware/.

[7] Anthony Schoettle, Hackers pounce as coronavirus spread triggers work-at-home movement, IBJ (March 13, 2020), https://www.ibj.com/articles/hackers-pounce-as-coronavirus-spread-triggers-work-at-home-movement.

[8] See Allison Grande, COVID-19 Warrants CCPA Enforcement Delay, Calif. AG Told, Law360 (March 19, 2020), available at https://www.law360.com/articles/1255181/covid-19-warrants-ccpa-enforcement-delay-calif-ag-told.

[9] Centers for Disease Control and Prevent, Coronavirus Disease 2019 (COVID-19), Interim Guidance for Businesses and Employers, available at https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html.

[10] Pub. L. No. 101-336 (relevant provisions codified at 42 U.S.C. § 12112(d)(3)(B); §12112(d)(4)(C)).

[11] Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 & 42 U.S.C.).122 Stat. 881.206(a).

[12] Pub. L. No. 111-84, 123 Stat. 124 (codified 29 C.F.R. § 825.500 (g)).

[13] The US Equal Employment Opportunity Commission, Pandemic Preparedness in the Workplace and the Americans with Disabilities, available at https://www.eeoc.gov/facts/pandemic_flu.html.

[14] 29 C.F.R. § 1630.14(c)(1)(i).

[15] The European Data Protection Board, Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak (March 19, 2020), available at https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en.

[16] *Id.*

[17] Under the GDPR, data regarding an individual's health, even body temperature, may be considered as a "special category" of personal data under the GDPR. In principle, the processing of such personal data is prohibited unless one of the exceptions listed in Article 9(2) of the GDPR applies. Processing of health data should generally comply with the specific rules set forth under the GDPR, but also with the additional requirements of each Member State, where applicable (Article 9(4), GDPR).

[18] Article 9(2)(i), GDPR.

[19] Article 9(2)(c), GDPR and recital 46 of the GDPR explicitly referring to the control of an epidemic.

[20] Including the following countries: Austria, Belgium, Bulgaria, Czech Republic, Denmark, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Lithuania, Luxembourg, Norway, Poland, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

[21] Article 6(1)(d), GDPR.

[22] Belgian data protection authority (APD), “COVID-19 et traitement de données à caractère personnel sur le lieu de travail” (March 13, 2020), available at https://www.autoriteprotectiondonnees.be/covid-19-et-traitement-de-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-sur-le-lieu-de-travail.

[23] French data protection authority (CNIL), “Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles” (March 6, 2020), available at https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles.

[24] Datenschutzkonferenz (DSK), “Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie” (March 13, 2020), available at https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5217154; cf. also Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, “Hinweise zum datenschutzgerechten Umgang mit Corona-Fällen” (March 13, 2020), available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/03/FAQ-Corona.pdf and Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, “Beschäftigtendatenschutz in Zeiten des Corona-Virus” (March 17, 2020), available at https://www.datenschutz.rlp.de/de/themenfelder-themen/beschaeftigtendatenschutz-corona/.

[25] Spanish data protection authority (AEPD), press release and report (March 12, 2020), available at https://www.aepd.es/es/documento/2020-0017.pdf.

[26] United Kingdom data protection authority (ICO), “Data protection and coronavirus” (March 12, 2020), available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/ and https://ico.org.uk/for-organisations/data-protection-and-coronavirus/.

[27] *Id.*

[28] *Id.*

[29] *Id.*

Gibson Dunn's lawyers are available to assist with any questions you may have regarding developments related to the COVID-19 outbreak. For additional information, please contact any member of the firm's Coronavirus (COVID-19) Response Team.

The following Gibson Dunn lawyers prepared this client update: In the US: Alexander H. Southwell, Ryan T. Bergsieker, Cassandra L. Gaedt-Sheckter, Daniel E. Rauch, and Lisa V. Zivkovic; in the EU: Ahmed Baladi, Patrick Doris, Michael Walther, Vera Lukic, Alejandro Guerrero, Kai Gesing, Selina Grun, and Clemence Pugnet. Gibson Dunn lawyers regularly counsel clients on the privacy and cybersecurity issues raised by this pandemic, and we are working with many of our clients on their response to COVID-19. Please also feel free to contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the Privacy, Cybersecurity and Consumer Protection Group:

United States
Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375,

jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe
Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation