

How COVID-19
continues to
affect data
privacy in
employment

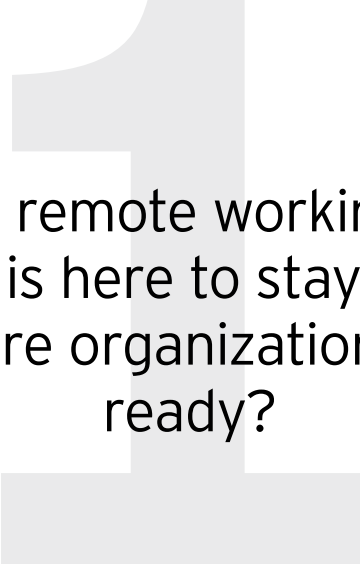


EY

Building a better
working world



More than a year after the start of the COVID-19 pandemic, the data privacy and employment law landscape continues to change and adapt to constant developments. While the discussion around the intricacies of remote working and government furlough schemes is ongoing, in many parts of the world, there is now additional focus on ways to return to the office, the role that vaccination programs play in this effort and the processing of employee personal data linked to COVID-19.



If remote working is here to stay, are organizations ready?

According to a survey carried out by Gartner, **82% of 127** company leaders, representing HR, Legal and Compliance, Finance and Real Estate, intend to permit remote working some of the time as employees return to the workplace.

With remote working being a necessity in some areas for more than a year now and with it possibly becoming a regular working pattern globally, the associated data privacy risks remain relevant. Organizations held much more control over their data when employees were mostly office-based. However, over the past year, they have had to adapt their remote working policies and reassess their technical and organizational measures to verify that data is adequately protected.

Encryption and pseudonymization are among the measures that are crucial for preventing a potential data breach, according to Article 32 of the General Data Protection Regulation (GDPR). Data breaches might be more likely to occur when employees work remotely and possibly connect to unsafe networks, use unauthorized devices or do not maintain adequate levels of data protection. Data mapping, verifying that third-party software is compliant and producing detailed remote working policies help confirm that employees are aware of risks, procedures and leading practices on accessing and handling personal data while working from home.

However, while these technical measures are crucial, according to the 2021 [Global EY Law Survey](#), a joint undertaking by EY Law and the Harvard Law School Center on the Legal Profession, 65% of general counsel do not believe they have the data or technology to respond to a data breach.

From an employment law perspective, regardless of whether the work is conducted at an office or employees' homes, the employer is responsible for the employees' working environment, including their health and safety. As such, remote working requires that employers put in place relevant policies and routines to confirm that work environment risks are assessed and regularly followed up to mitigate risk factors. Risk assessments of the work environment at an organizational level must also involve any appointed employee safety representatives.

This obligation may trigger an increased burden of responsibility on legal, compliance and HR departments. The Global EY Law Survey shows that law departments face rising volumes of work, with 75% of general counsel expecting workloads to outpace budgets over the next three years.

While remote working remains a current and future topic, discussions around a potential return to the office are underway in many organizations. The Global EY [Return to Office Tracker](#) navigates the existing legal framework for returning to the office, enforceability of employment contract obligations and employee rights and obligations across jurisdictions.

Things to consider:

- ▶ Going forward, employers that continue to allow their employees the flexibility to work from home full-time or part-time will need to verify that high privacy and security standards are maintained in and out of the office.
- ▶ According to the 2021 Global EY Law Survey, 65% of general counsel do not believe they have the data or technology to respond to a data breach.
- ▶ Such employers need to bear in mind that they remain responsible for the employees' working environment, including their health and safety.

COVID-19 and employee health data

Since the start of the COVID-19 pandemic, employers have been faced with new challenges on collecting and processing employee personal data. Employers have had to ask their employees more questions than usual, first due to employee access to the workplace during the pandemic and then as part of plans for a widespread return to the office and to cooperate with wider track-and-trace efforts. HR personnel and health screening questionnaires have posed sensitive questions covering potential virus contraction, vaccination information and travel plans.

Additionally, as the employer is legally responsible for providing a safe and healthy working environment, adequate actions had to be taken to safeguard individuals from infection at the workplace. This includes an obligation for employees to inform the employer whether they are or have been infected or are at risk of being infected.

According to Article 9 of the GDPR, processing personal health data is generally prohibited. However, Article 9 provides exceptions in relation to processing that are deemed necessary either for exercising rights and obligations of the controller or the data subject in the field of employment or for reasons of public interest in the area of public health.

This means that, while employee consent is required to collect and process sensitive personal data to the extent the data is essential to meet the purposes of the employment relationship, employers can lawfully request disclosure and processing of employees' health data by virtue of the existing employment relationship or for reasons of public interest, including the COVID-19 pandemic. The European Data Protection Board has expressed the opinion that the imbalance of power in the employment relationship renders employees' consent invalid. However, in line with Articles 9 and 15 of the GDPR, employees have a right to obtain confirmation from the employer as to whether their personal data is being processed and can request access to the purposes of processing, the categories of personal data held, the recipients of such data and the associated retention period.



Further, Article 6 of the GDPR provides two additional lawful bases for the processing of health-related personal data: to comply with a legal obligation to which the controller is subject or to protect the vital interests of either the data subject or another natural person. Again, this would mean that employers can justify the processing of such sensitive personal data on the basis that vital interests of their personnel are at stake or on the basis of the employers' duty to protect the health, safety and welfare of their employees.

In comparison, the California Consumer Privacy Act does not specifically list the legal reasons that organizations can process personal data, and it notably limits the right of access for employees. While this was expected to change, the California Privacy Rights Act extended this exception to January 2023.

Can the employer force vaccination?

Under the above rules, employers can ask whether an employee has been vaccinated but cannot generally request that employees get vaccinated. However, special considerations may be needed depending on the type of work that will be carried out. Based on the legal position as reported in the jurisdictions included in the Global EY [Return to Office Tracker](#), most jurisdictions indicate that employers cannot mandate vaccinations for their employees. In certain jurisdictions, there is no definitive right for employers to mandate a vaccine, but the law stipulates that they must consider several factors, including the industry or sector in which they operate and whether such a condition would be reasonable.

Several jurisdictions, for example, indicate that health care workers could reasonably expect to be obligated to obtain a vaccination. Only a few jurisdictions report that the employer may bear the burden of funding the vaccine directly; it is more likely that, according to government policy to promote mass vaccination, employers will be obligated to allow employees paid leave to attend public health centers to be vaccinated. The Global EY [Return to Office Tracker](#) navigates the existing legal framework in more than 60 jurisdictions.

Generally, employees cannot be dismissed on the basis that they refused to get vaccinated. This could, however, change if a statutory vaccination requirement is introduced.

Things to consider:

- ▶ Employees need to disclose more health data than usual to their employers in the name of public health. However, employees in Europe retain their right to ask their employer how and why data is being processed.
- ▶ Employers cannot force employees to be vaccinated based on their contractual relationship, but this could happen if a statutory requirement is introduced.

How furlough and redundancies resulted in a spike in data subject access requests

According to a survey* among 100 UK-based data protection officers (DPOs) in organizations of 250 employees or more, 30% of respondents expect a significant increase in data subject access requests (DSARs) once the pandemic is over. The reason for this expected spike in DSAR submissions can be found in the widespread use of furlough schemes and in mass redundancies that have been taking place due to the pandemic.

While there may be significant differences in approach across jurisdictions, the EY [Labor and Employment Law Tracker](#) provides a current snapshot of legal considerations with regard to employer rights and obligations, government furlough and incentive schemes as well as relevant topics of workforce transformation.

As employers are obliged to keep their employees' personal data safe, secure and up to date, building a robust DSAR workflow is critical to handle increased employee requests for access to their data. It starts with knowing what types of data are being held and how to access the data, a process that can be painful if a data-mapping exercise has not taken place. Data mapping confirms that each data type is used only for its original purpose and that it is not retained beyond the necessary point.

Technology plays a significant role in DSAR intake and identity verification, data redaction, data encryption for secure delivery and case management. Carefully selecting technology solutions for each part of the process will provide quick turnarounds to comply with regulatory deadlines, reduced cost and increased scalability.

While technology offers numerous solutions to privacy topics including DSARs, respondents to the 2021 Global EY Law Survey ranked data privacy and cybersecurity risks as "8 out of 10" compared with the other risks facing the organization in the next 12 months. This indicates that many organizations are still searching for right strategy to deal with privacy compliance and risk management.

* Survey conducted by Sapio Research for Guardium between 29 April and 5 May 2020.

Things to consider:

- ▶ Respondents to the 2021 Global EY Law Survey ranked data privacy and cybersecurity risks, as “8 out of 10” on a scale where 10 signifies an important business risk, compared with other risks facing organizations in the next 12 months, with DSARs being a common area of concern.
- ▶ A detailed DSAR workflow that provides a timely and compliant treatment of incoming requests is crucial and can make life easier for organizations.

4

Transferring employee data post-Schrems II

In cases where employee personal data needs to be transferred and processed across borders, additional considerations come into play. In particular, the recent Schrems II decision* by the European Court of Justice deemed the EU-US Privacy Shield to be an inadequate mechanism to enable data transfers to the US under EU law as it doesn't provide an adequate level of protection, essentially equivalent to that guaranteed within the EU by the GDPR.

This decision has impacted numerous businesses that conducted transatlantic trade solely on the basis of this adequacy decision and were instructed to immediately stop processing personal data and institute another approved transfer mechanism, such as standard contractual clauses (SCCs). The decision also introduced the obligation for a case-by-case assessment of SCCs to confirm that adequate protection is provided. The Court specified that the protection assessment must consider both the SCCs agreed between the EU data exporter and the data importer established in a third country, as well as any access by the public authorities of that third country and the relevant aspects of the country's legal system (e.g., existing enforceable rights and effective legal remedies for data subjects).

Considering the amounts of employee personal data that are being transferred from the EU to the US, often by large multinationals headquartered in the US with workforces in the EU, the implications of the Schrems II decision on employers are significant. Organizations need to continue identifying any data transfers that in the past would rely on the Privacy Shield and put alternative measures in place.

* Judgment in Case C-311/18, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*.

Things to consider:

- ▶ Months after being issued, the Schrems II decision continues to cause headaches to organizations, including US employers with workforces based in the EU.
- ▶ While the EU and the US continue discussions about a potential future arrangement that will replace the Privacy Shield, organizations need to continue identifying affected data transfers and using alternative means of transfer, including a case-by-case application of SCCs.

Adaptations to data privacy and employment law have been commonplace since the beginning of the COVID-19 pandemic. With a future involving an expected mix of remote and in-office work, the role vaccinations will play and the processing of employee data related to COVID-19, employers and employees will continue to be faced with change.



Contacts



Meribeth Banaschik
Partner, Forensic & Integrity Services
meribeth.banaschik@de.ey.com



Paula Hogeus
EY Global Labor and Employment Law Leader
and Nordics Law Leader
paula.hogeus@law.se.ey.com



Hanna Julin
Manager, EY Global Labor and Employment Law
hanna.julin@law.se.ey.com



Kalliopi Kakaletri
Manager, Forensic & Integrity Services
kalliopi.kakaletri1@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2021 Ernst & Young LLP
All Rights Reserved.

EYG no. 007033-21Gbl
2105-3780246
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com