Hogan Lovells

Managing Workforce Cyber Risk in a Global Landscape: A Legal Review

Fifteen-country analysis by global law firm Hogan Lovells illustrates how workforce monitoring can be deployed internationally for insider threat management

By:
Harriet Pearson, Washington, D.C. & New York
James Denvil, Washington, D.C.

Sponsored by

FORCEPOINT
POWERED BY Raytheon

EXECUTIVE SUMMARY[1]

Numerous recent events have shown how cyber incidents can cripple operations, damage reputation, and expose organizations to regulatory consequences and private litigation. To effectively identify, prevent, and mitigate the effects of cyber incidents, organizations need to address both external and internal threats.

Your organization's workforce is one source of risk in this context. Whether due to inadvertent or malicious activities, your workforce may expose your assets and information systems to compromise. In fact, a recent study has shown that over half of cyber incidents are caused by insider threats. One of the ways to mitigate this risk effectively is to monitor the use of information resources. Doing so can provide insight into what constitutes routine use, making it easier to identify anomalies. And that can help organizations detect potential cyber incidents and act to prevent them or address them more quickly if they do occur.

While workforce monitoring of this type promises substantial benefits for cyber risk management, there are legal compliance issues to be considered, particularly when such cyber defense programs are deployed internationally.

Workforce monitoring activities are governed by a variety of data protection, data privacy, communications secrecy, and employment laws. Some jurisdictions may permit organizations to engage in a broad range of workforce monitoring activities, without requiring organizations to undertake substantial compliance efforts. However, other jurisdictions may restrict the scope of monitoring, perhaps requiring organizations to collect and process only metadata unless there are reasonable suspicions of serious misconduct. And some jurisdictions may require organizations to consult with workforce representatives, obtain consent from workforce members, or notify government authorities of monitoring activities.

It is possible to navigate these requirements efficiently, once they are identified and when aided by flexible tools that can be tailored to help meet the requirements of local law.

In Parts I and II of this white paper, we provide an overview of the legal issues associated with such workforce monitoring programs. Part II also includes a Table that summarizes the relative degree of compliance effort required to deploy various elements of such a program in fifteen selected countries, characterizing the overall level of effort as "Basic," "Moderate," or "Significant." Drawing on our experience advising clients globally on these issues, in Part III we describe some leading practices that organizations can adopt to support the development of effective programs. And in Part IV we present high-level summaries of the workforce monitoring legal frameworks in each of 15 countries.

We hope that this white paper proves a useful guide to those charged with reviewing and refining their organization's compliance programs in light of the increasing need for situational awareness of threats to IT systems and data.

[1] Special thanks to Peter Leonard (Australia), Melissa Fai (Australia), Mark Hayes (Canada), Adam Jacobs (Canada), Mikko Manner (Finland), Tuulia Karjalainen (Finland), Janina Tahvanainen (Finland), Sonja Heiskala (Finland), Winston Maxwell (France), Patrice Navarro (France), Alexandra Tuil (France), Mathilde Gérot (France), Tim Wybitul (Germany), Wolf-Tassilo Böhm (Germany), Lukas Ströbel (Germany), Marco Berliri (Italy), Massimiliano Masnada (Italy), Giulia Mariuz (Italy), Joke Bodewits (Netherlands), Chantal van Dam (Netherlands), Zechariah Chan (Singapore), Leishen Pillay (South Africa), Gonzalo Gállego (Spain), Paula García (Spain), Niklas Sjöblom (Sweden), Andreas Hakamaa (Sweden), Julia Bhend (Switzerland), Kayra Üçer (Turkey), Tolga İpek (Turkey), and Eduardo Ustaran (United Kingdom) for their assistance in the review of relevant laws around the world.

I. Introduction

Cyber incidents pose substantial business and legal risks to your organization. If bad actors access your systems, networks, or information, the fallout could damage your organization's reputation, diminish customer loyalty, hurt partner relationships, and negatively impact stock price or market value. You could find yourself facing government investigations, regulatory consequences, and private litigation.

To manage cyber risk effectively, your organization needs to have the ability to detect, prevent, and investigate cyber incidents.[2]

Some may think this means that you need to focus on threats coming from outside your network—scanning for signs that bad actors are attempting to gain or have succeeded at gaining access. This is true, of course. However, it has been found that 55 percent of all cyber attacks are the result of malicious or inadvertent workforce actions.[3]

Generally speaking, to detect and protect against workforce threats, you need to learn how your workforce uses your assets, identify anomalies associated with potential unauthorized activities, and implement controls designed to prevent or detect incidents. The tools to address workforce threats may involve, among other things:

- Monitoring temporal metadata (e.g., logon, logoff, session length)
- Monitoring use of privileged access, such as to administrative accounts
- Monitoring use of applications
- Monitoring email communications
- Monitoring employer-provided devices
- Monitoring Internet browsing
- Capturing on-screen activities
- Keylogging
- Monitoring behavior on social media and other channels
- Monitoring employee-owned devices

The activities listed above require monitoring workforce use of information technology resources. In doing so, you might collect and process personal information related to your workforce, you could capture private communications sent or received by your workforce, and you may collect information that could allow you to evaluate workforce efficiency. As such, cyber defense programs may end up collecting and processing information in ways that implicate laws or regulations governing privacy and data protection, communications secrecy, or employment. These laws and regulations are far from consistent around the world.

Programs may end up collecting and processing information in ways that implicate laws or regulations governing privacy data protection, communications secrecy, or employment.

In some jurisdictions, organizations have broad authority to monitor workforce use of information assets. In others, organizations may need to avoid processing personal communications, analyze private communications and information only where there are reasonable suspicions of misconduct, consult with workforce representatives, or obtain consent from workforce members. In the United States, for example, federal law provides that organizations are exempt from liability to the extent that they monitor their information systems for cybersecurity purposes. But in Finland, employers are generally prohibited from accessing the contents of communications sent to or received by employees.

[2] Major industry-level standards and frameworks recognize the need for such monitoring. See, for example, the ISO 27000 family of information security management standards and the U.S. National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (also known as the "NIST Cybersecurity Framework") at pp. 30-32, available respectively at https://www.iso.org/isoiec-27001-information-security.html (for purchase) and https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[3] Nick Bradley, *The Threat Is Coming from Inside the Network: Insider Threats Outrank External Attacks*, SecurityIntelligence (June 1, 2015), https://ibm.co/1QAAIiu.

Developing, deploying, and maintaining an effective and legally compliant global insider threat program of this type, therefore, requires a practical understanding of applicable laws and tools that can be adapted to varying circumstances and compliance frameworks. This paper is the first published review of the international legal landscape of which we are aware that specifically addresses cyber-focused workforce threat program implementation, and may thus be helpful as a high-level guide.

II. Legal Considerations for Workforce Monitoring Programs

As discussed in the Introduction, there are substantial differences in the legal frameworks governing the monitoring of workforce use of information technology resources. Some jurisdictions permit organizations to engage in broad monitoring of workforce activities, emphasizing the importance of mitigating cyber risk. Other jurisdictions restrict organizations' monitoring activities, reflecting an emphasis on respecting privacy interests or labor rights of the workforce. In this section, we summarize some of the legal issues that may affect cyber defense programs.

In general, there are three areas of law that govern cyber defense programs that involve monitoring of workforce activities: data privacy and data protection laws; communications secrecy laws; and employment laws.

Data privacy and data protection laws

When monitoring workforce activities for signs of workforce threats, organizations often will collect some types of personal information (i.e., information that on its own or in combination with other information links or is reasonably linkable to a particular individual). The collection and processing of such information may be governed by data privacy and data protection laws. In most of the jurisdictions reviewed for this white paper, the guiding principle for evaluating employee workforce monitoring activities under data privacy or data protection laws is reasonableness. Organizations generally may engage in monitoring activities that reasonably address cyber risks in a manner that reflects a reasonable balance between workforce privacy interests and the organizations' interests in managing cyber risks.

In general there are three areas of law that govern cyber defense programs that involve monitoring of workforce activities: data privacy and data protection laws, communications secrecy laws, and employment laws.

To assess the reasonableness of implementing a particular insider internal threat tool or other measure, organizations can ask the following questions:

- Is the deployment of the tool or measure intended to address an identified cyber risk?
- Will use of the tool or measure effectively address the identified risk?
- Are there other tools or measures that could effectively address the risk in a manner that would have less of an impact on the privacy interests of workforce members?
- Will the impact on the privacy interests of workforce members outweigh the benefits to the organization?

In other words, to address data privacy and data protection laws, organizations should consider whether they can articulate their reasons for deploying monitoring tools and demonstrate that the tools or other measures being used reasonably support those objectives without unduly impacting privacy interests.

Recent guidance from the Article 29 Working Party, which includes representatives from all European Union ("EU") Member States, provides some insight into how data protection authorities expect organizations to conduct such assessments.[4] The guidance recognizes that monitoring technologies can help employers protect company assets and information held or processed by companies, while noting that the regulators believe that the technologies pose "significant privacy and data protection challenges."[5] The guidance also includes examples of how data protection authorities would assess certain types of workforce monitoring activities.

[4] Article 29 Working Party, Opinion 2/2017 on data processing at work (2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

[5] *Id.* at 4.

For example, the Working Party considers an organization's deployment of a tool that would decrypt and inspect all information traveling across the organization's network. Such a tool might be deployed to address the identified risks of data leakage and malicious attempts to gain unauthorized access to networks. And the tool might be effective at addressing those risks. However, the Working Party suggests that monitoring all online traffic might be a disproportionate response to the identified risks and recommends that organizations assess whether less intrusive tools might be as effective at addressing the risks. If less intrusive tools are not as effective or are not available, the Working Party advises that the tool should be deployed in a manner that will reduce the potential privacy impact. Privacy safeguards could include:

- Blocking, rather than logging, suspicious traffic. Users could be directed to a portal where they could review the determination and request that information be released if appropriate.
- Using automated tools to detect anomalies in workforce use of information systems that are associated with specified threats, and flagging activities for review only where anomalies are found.
- If logging is necessary, recording the minimum amount of information needed to address the identified risks.
- Providing workforce members with unmonitored Internet access via secure channels to support private communications.
- Disabling the monitoring of communications involving online banking or health platforms.
- Providing workforce members with clear information about the types of monitoring that will be conducted.
- Providing workforce members with clear information about the types of activities that may lead to the access and review of communications.
- Deploying the tool so that it prioritizes the prevention of misuse rather than the detection and recording of misuses (e.g., warning workforce members that they may be about to violate applicable policies rather than recording that workforce members have violated such policies).

The guidance recommends that organizations prioritize preventing inadvertent and intentional misconduct over detecting such activities. If blocking access to certain web sites or other online services effectively addresses a specified threat, the regulators advise that it would not be reasonable for organizations to record workforce internet use for purposes of addressing that threat.[6]

It must be emphasized that the test of reasonableness is highly fact-specific. Whether a particular measure is reasonable will depend, among other things, on the sensitivity of the information collected, the nature of the systems that are being protected, the nature and severity of the threats facing the organization, and the laws and regulations to which the organization is subject. Organizations should therefore consider documenting their assessments of workforce monitoring tools to demonstrate efforts to comply with applicable laws.

Regulators advise that organizations provide their workforces with clear notices regarding monitoring, including information about acceptable use of company resources. The importance of such transparency is underlined in a recent ruling from the European Court of Human Rights in which Romanian courts were faulted for not adequately considering whether an employee received sufficient notice of the monitoring of his personal communications.[7]

Whether monitoring captures the personal information of workforce members located in the EU or elsewhere, organizations should confirm that they comply with their data privacy and data protection obligations. Depending upon the jurisdiction, those requirements may include, among other things, obtaining consent, providing transparent notices, limiting storage of and access to personal information, and registering with data protection authorities.

Organizations with workforce members in the EU should also be mindful of the EU General Data Protection Regulation ("GDPR"), which takes full effect on May 25, 2018. The GDPR includes, among other things, new accountability obligations for companies that process personal information, stronger rights for individuals, and requirements for organizations to conduct written data protection impact assessments prior to deploying monitoring tools in some cases. GDPR compliance obligations are substantial, and there is little compliance guidance available for some of the requirements. There is hope that good faith, documented efforts to comply will reduce the risk of unwanted regulatory scrutiny. However, organizations should recognize that violations of the GDPR could expose them to fines of up

[6] *Id.* at 23.

[7] Tim Wybitul & James Denvil, *European Court Proposes Criteria for Assessing Employee Monitoring Activities*, Chronicle of Data Protection (Sept. 8, 2017), http://bit.ly/2gSVrKd.

to the higher of €20 million or four percent of annual worldwide turnover. And though the GDPR is intended to harmonize data protection laws across the EU, organizations will still need to be mindful of the laws in individual Member States. The GDPR permits Member States to adopt specific rules regulating the processing of personal information in employment contexts.

Communications secrecy laws

Monitoring workforce use of electronic communications networks and tools can be an essential part of an effective cyber defense program. Malicious or inadvertent actors may use communications networks or tools to transmit sensitive information outside of protected environments or to download malware or other malicious software that could compromise employer assets and information. Monitoring the use of communications networks and tools can help organizations prevent the transmission or download of such information and detect signs of unauthorized activities.

Many jurisdictions have adopted laws that restrict the interception or recording of the contents of communications while in transit on communications networks, including networks owned or operated by employers. These laws typically permit organizations, or other parties, to intercept or record the contents of a communication if at least one party to the communication consents, with some jurisdictions requiring the consent of all parties. And some jurisdictions permit organizations to intercept or record the content of communications without consent, provided that the activities are focused appropriately on addressing network security. Consent can sometimes be implied based on the issuance of clear notices alerting workforce members to the deployment of monitoring tools. But some jurisdictions may require express consent.

Violating communications secrecy laws can result in substantial financial penalties, or even criminal sanctions, in some jurisdictions. Organizations that wish to deploy cyber defense programs that involve monitoring the contents of communications should therefore assess the application of communications secrecy laws and develop appropriate compliance mechanisms.

Employment laws

Some jurisdictions require that organizations consult with or obtain consent from, employee representatives (e.g., works councils) prior to deploying tools that monitor employee activities. These interactions can be time consuming, and organizations should allow for adequate time to meet with employee representatives and finalize needed agreements. Organizations also need to assess whether they need to obtain approval from, or register monitoring programs with employment authorities prior to monitoring for insider threats. In Italy, for example, organizations generally must enter into agreements with trade union representatives or obtain authorizations from the local employment office before monitoring employee activities.

These considerations may come as a surprise if the stakeholders developing cyber defense programs all reside in jurisdictions that lack such employment laws. To avoid overlooking these and other global issues, organizations with global workforces may want to consider convening multi-jurisdictional teams to develop and discuss insider threat programs and their supporting compliance programs.

Table. Legal Compliance Effort to Implement Workforce Monitoring for Cyber Risk Management

(rated on scale of 1 to 5, from basic to more significant levels of effort)

	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	Switzerland	United Kingdom	Australia	Canada	Singapore	South Africa	Turkey	United States
Compliance Effort *Overall*[8]	*Significant*	*Significant*	*Significant*	*Significant*	*Moderate*	*Moderate*	*Moderate*	*Significant*	*Moderate*	*Basic*	*Moderate*	*Basic*	*Basic*	*Moderate*	*Basic*
Monitoring temporal metadata (e.g., logon, logoff, session length)	3	3	4	4	1	2	2	2	1	1	1	2	2	1	1
Monitoring use of privileged access (e.g., administrator accounts)	3	3	3	3	2	2	2	3	2	1	2	1	2	2	1
Monitoring use of applications	5	3	4	4	2	2	2	4	2	1	2	1	2	2	2
Monitoring email communications	5	4	4	4	3	3	3	4	3	2	3	2	2	3	2
Monitoring employer-provided devices	5	4	4	4	3	3	3	4	3	2	3	2	2	3	2
Monitoring Internet browsing	5	4	4	5	4	4	3	4	4	2	3	2	2	3	2
Capturing on-screen activities	5	5	5	5	4	4	4	5	3	2	4	4	2	4	2
Keylogging	5	5	5	5	5	4	4	5	5	2	4	4	2	4	2
Monitoring behavior on social media and other channels	5	5	4	4	5	4	4	5	5	4	4	2-4	4	4	3
Monitoring employee-owned devices	5	5	5	5	4	5	5	4	4	4	4	4/5	4	4	3
Total	46	41	42	43	33	33	32	40	32	21	30	24-27	24	30	20

[8] ***Compliance Effort Overall*** is an approximate characterization of the level of compliance resources required to implement a comprehensive workforce monitoring program for cyber threat management in a particular country. A total of up to 29 points is characterized as requiring a "Basic" level of compliance resources; between 30 and 39 is "Moderate"; and 40 and up is "Significant." These ratings are provided for illustrative purposes only. For more information, consult the detailed descriptions in Section IV of this paper. It should be noted that not all elements of such a monitoring program are required to be implemented in order for an organization to have an effective cyber risk management program.

III. Leading Practices

Developing and maintaining a global, effective, legally compliant cyber defense program can seem daunting. Administrative requirements and conflicting laws sometimes seem to work against the need to establish effective operational procedures. But there are steps organizations can take to make it easier to navigate these challenges.

Identify the threats you want to address

In many jurisdictions, the lawfulness of monitoring will depend, at least in part, upon whether the monitoring addresses reasonable threats. Identifying and articulating the specific threats you wish to address will support the compliance analysis and help you choose the right tools for the job. Designing a cyber defense program to address "all cyber incidents that may impact the company" would be a daunting, if not impossible task. Designing a program to address "the unauthorized exfiltration of restricted access information via e-mail" and other specified threats will be far more manageable. And it will be easier to identify and develop the compliance mechanisms needed to support the program.

Identify the jurisdictions involved

Once you have identified the threats you are looking to address, it may be tempting to start choosing the most efficient tools for the job. However, doing so may be premature. Keyloggers may be an effective tool for detecting unauthorized activities when workforce members have access to sensitive systems. But some jurisdictions may prohibit the use of keyloggers in all or nearly all circumstances. Identifying the jurisdictions in which you will engage in monitoring helps to focus the design of insider threat programs by identifying the legal frameworks in play.

Convene a cross-functional, multi-jurisdictional team to assess operational and compliance considerations

To support the selection of tools and the development of the compliance framework, employers may want to convene a cross-functional team. Such a team could be comprised of representatives from across the business, including Information Security, Legal, Compliance, and Human Resources. And it may be useful to include representatives from a number, if not all, of the affected jurisdictions. Such a team can help organizations design cyber defense programs that mitigate risk while aligning with the company's culture and operational realities. If cyber defense programs are designed by stakeholders from a single business unit located in just one jurisdiction, there is a risk that the program will fail to align with the company's global culture and fail to support operational realities. And convening a cross-functional, multi-jurisdictional team may make it easier to identify and assess the broad range of compliance requirements that may need to be addressed.

Develop policies

Once organizations have chosen the tools they wish to use and determined how they want to use them, they should develop the policies needed to support the deployment of the tools. Such policies should, among other things, establish roles and responsibilities for managing and operating cyber defense programs, limit authorized access to monitoring information in a manner that aligns with applicable laws while supporting program goals, and establish retention and disposal requirements for monitoring information.

Address compliance

Depending upon the jurisdictions involved, organizations may need to address a range of compliance requirements, including implementing monitoring tools so that they only capture aggregate information, avoiding the processing of private communications or files, obtaining consents from workforce members, consulting with employee representatives, obtaining authorizations from government authorities, and addressing international data transfer requirements. Choosing tools that can adapt to jurisdictional restrictions (e.g., allowing organizations to disable the monitoring of contents in some jurisdictions) can be very helpful.

Finally, in jurisdictions in which the relevant requirements are not already understood or clear, organizations seeking to develop compliant policies and address compliance requirements may wish to seek advice and assistance from counsel familiar with applicable data privacy and data protection, communications secrecy, and employment laws. Experienced counsel can help organizations avoid the potential legal risks of deploying cyber defense programs in a non-compliant manner while providing practical advice about how to address the administrative hurdles posed by consultation and authorization requirements.

IV. Country Requirements

In this section, we summarize the general requirements for workforce monitoring programs in fifteen jurisdictions. These summaries are not intended as legal advice, and the analysis may not apply to the factual or legal circumstances that you or other organizations are facing. Organizations that wish to implement cyber defense or other workforce monitoring programs in these jurisdictions are advised to consult with competent attorneys licensed to practice in the applicable jurisdictions.

The countries we summarize are, in order of presentation:

- Finland
- France
- Germany
- Italy
- Netherlands
- Spain
- Sweden
- Switzerland
- United Kingdom
- Australia
- Canada
- Singapore
- Turkey
- United States

FINLAND

General considerations. Finland imposes strict limitations on monitoring employees' use of communications tools.

Employers may use automated tools to monitor traffic data of electronic communications (i.e., communications metadata) on an aggregate level that does not enable the identification of individuals for the purposes of preventing or investigating: the disclosure of trade secrets; the installation of unauthorized devices, services, or software on employer networks; unauthorized access to employer networks; and similar misuse of employer resources as defined in acceptable use policies presented to employees.

In limited circumstances—such as where automated monitoring indicates an anomaly or there are other reasonable grounds to believe that an important trade secret has been disclosed or that employer networks have been misused in a manner that likely would cause substantial harm to the employer—employers may manually review traffic data associated with employee communications. Employers must document each instance of manual review in writing. And the written report must be provided to the affected employees once such disclosure will not compromise the investigation. Employers must notify the Finnish Data Protection Ombudsman (*Fin. tietosuojavaltuutettu*) and employee representatives before implementing monitoring programs. And employers must provide those entities with annual reports of manual reviews.

Employers may not monitor the contents of electronic communications.

Employers may monitor employee access to and use of databases and applications that do not contain contents of communications or traffic data if the monitoring is conducted for legitimate purposes that are not outweighed by the potential adverse impact on employees; the monitoring is transparently disclosed to employees; and the monitoring is necessary for managing the rights and obligations associated with the employment relationship.

Notification Considerations	Consent Considerations
For monitoring that involves the processing of personal data, employers must provide clear information about: (1) the purposes of collecting personal data; (2) the potential recipients of personal data; (3) employees' rights regarding personal data; and (4) contact information for entities controlling processing of the data. Employers must also provide information about acceptable use of resources.	Consent does not serve as a lawful basis for monitoring employee activities. Instead, monitoring can proceed under the conditions described above.

Additional Considerations. Organizations that employ 30 or more employees must consult with employees or their representatives before engaging in monitoring activities, as set forth in the Act on Cooperation within Undertakings (334/2007).

Under the GDPR, employers likely will have to conduct a data protection impact assessment prior to engaging in monitoring. Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access or delete data and data transfer restrictions.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws and Regulations. Personal Data Act (523/1999); General Data Protection Regulation (effective May 25, 2018); Information Society Code; Act on the Protection of Privacy in Working Life; Employment Contracts Act (55/2001).

Finland: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	3: *Estimate based on engagement with employee representatives.*
Monitoring use of privileged access (e.g., administrator accounts)	3: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	5: *Strict limits on the monitoring of communications tools.*
Monitoring email communications	5: *Limited to traffic data for specific purposes.*
Monitoring employer-provided devices	5: *Strict limits on processing communications data. Other processing of personal data must be necessary for managing the employment relationship.*
Monitoring Internet browsing	5: *Limited to traffic data for specific purposes.*
Capturing on-screen activities	5: *Strict limits on processing communications data. Other processing of personal data must be necessary for managing the employment relationship.*
Keylogging	5: *Processing of personal data must be necessary for managing the employment relationship.*
Monitoring behavior on social media and other channels	5: *Processing of personal data must be necessary for managing the employment relationship.*
Monitoring employee-owned devices	5: *Strict limits on processing communications data. Other processing of personal data must be necessary for managing the employment relationship.*

Employers may use automated tools to monitor traffic data of electronic communications (i.e., communications metadata) on an aggregate level that does not enable the identification of individuals for the purposes of preventing or investigating: the disclosure of trade secrets; the installation of unauthorized devices, services, or software on employer networks; unauthorized access to employer networks; and similar misuse of employer resources as defined in acceptable use policies presented to employees.

FRANCE

General considerations. As in other EU Member States, monitoring that involves the processing of personal data must satisfy the test of reasonableness. This test involves determining whether monitoring effectively achieves a reasonable business purpose in the least intrusive way without being outweighed by the impact on employees' privacy. Reasonable business purposes include detecting and preventing criminal activity or similarly serious misconduct. Monitoring or broadly sampling actual communications and similar activities generally will be viewed as being more intrusive than the use of automated monitoring tools that trigger alerts or otherwise prompt limited reviews by trained authorized users.

However, French data protection law and the right of privacy generally prohibit employers from accessing communications or information clearly marked "personal" unless employers have a court order, the employee is present or invited to be present when the communications are accessed, the information is accessed in association with judicial proceedings, or there is an emergency.

If monitoring tools are not used to capture personal data (e.g., in certain types of system logging), such use of the tools is not subject to the restrictions of data protection law.

Notification Considerations	Consent Considerations
Employers must provide employees with a clear information technology use policy that informs employees about: (1) the types of personal data that may be collected; (2) the purposes of collection; (3) how the data will be used; (4) the retention of personal data; and (5) the recipients, if any, of the personal data. Documents that contain the rules for acceptable use of company resources, the violation of which could result in sanctions imposed on employees, must be submitted to the Labor Inspector.	Consent does not serve as a lawful basis for the processing of employees' personal data because of the presumption that employees cannot freely give their consent. Consent is not required for monitoring that does not capture personal data or that is conducted in a manner that complies with the requirements described under general considerations.

Additional Considerations. Prior to deployment, employers should assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Notably, such an assessment will be required under GDPR. Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access, correct, or delete data, and data transfer restrictions. Employers should retain personal data captured via monitoring for no more than six months.

Employers must notify the French data protection authority ("CNIL") prior to deploying automated monitoring tools that capture personal data. Most notification obligations will cease to exist after GDPR takes full effect on 25 May 2018. However, authorization requirements may survive. Employers must consult with works councils that may be established in the work place before introducing new monitoring technologies.

Employers should avoid capturing employees' sensitive data information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history) unless there is a legal obligation to process the information.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. French Data Protection Act; General Data Protection Regulation (effective May 25, 2018); French Labor Code.

Employers should avoid capturing employees' sensitive data information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history) unless there is a legal obligation to process the information.

France: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	3: *Metadata only. Prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Monitoring use of privileged access (e.g., administrator accounts)	3: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access. Prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Monitoring use of applications	3: *Metadata only. Prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Monitoring email communications	4: *Avoid personal communications. Prior consultation with all competent staff representatives; file with data protection authority; provide employees with notice; and submit documents to the Labor Inspector.*
Monitoring employer-provided devices	4: *Avoid personal communications. Prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Monitoring Internet browsing	4: *Prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Capturing on-screen activities	5: *Need strong justification to demonstrate that the substantial impact on privacy is warranted as set forth by Article L.1121-1 of the French Labor Code. In such exceptional circumstances, prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Keylogging	5: *Need strong justification to demonstrate that the substantial impact on privacy is warranted as set forth by Article L.1121-1 of the French Labor Code. In such exceptional circumstances, prior consultation with all competent staff representatives; file with CNIL; provide employees with notice; and submit documents to the Labor Inspector.*
Monitoring behavior on social media and other channels	5: *Employers generally cannot monitor private conduct. However, employers may be permitted in exceptional circumstances to conduct monitoring tailored to alert employers to activities or behaviors that might cause serious harm to the company.*
Monitoring employee-owned devices	5: *Estimate based on likely need for separation of work and personal environments for monitoring and wiping. Employers may not access or monitor private applications or private use of communications resources.*

GERMANY

General considerations. If employers prohibit all personal use of electronic communications tools or allow personal use only if employees consent to monitoring, employers may engage in reasonable monitoring of the use of electronic communications resources, including Internet access. Otherwise, according to German data protection authorities, the Telecommunications Act generally prohibits employers from monitoring the contents of communications absent employee consent. To date, high courts in Germany have not addressed whether the data protection authorities' interpretation is correct. However, in recent years, some labor and administrative courts have ruled that employers may engage in some monitoring even if they permit private use of electronic communications tools.

As in other EU Member States, monitoring that involves the processing of personal data must satisfy the test of reasonableness. This test involves determining whether monitoring effectively achieves a reasonable business purpose in the least intrusive way without being outweighed by the impact on employees' privacy. Reasonable business purposes include detecting and preventing criminal activity or similarly serious misconduct. But detailed monitoring of user activities for those purposes will likely be viewed as disproportionate absent concrete suspicions of misconduct.

But detailed monitoring of user activities for those purposes will likely be viewed as disproportionate absent concrete suspicions of misconduct.

Monitoring for other purposes may or may not be considered to have a disproportionate impact on employee privacy interests–it depends on whether and how the monitoring captures personal data. Sampling communications or other activities generally will be viewed as being more intrusive than the use of automated monitoring tools. If monitoring tools do not capture personal data, the tools are not subject to the restrictions of data protection law.

Notification Considerations	Consent Considerations
Employers must provide employees with clear notice about: (1) the types of personal data that may be collected; (2) the purposes of collection; (3) how the data will be used; (4) the retention of personal data; (5) the recipients, if any, of personal data; and (6) name and contact details of the controller (i.e., the employer). If employers obtain consent to monitoring, such notice must be included in the employees' consent declaration form. A separate notice is not required in these circumstances.	Consent can serve as the basis for reasonable monitoring activities that involve the capture of personal data so long as employees have a clear, free choice. For example, consent will be a lawful basis for monitoring if employees consent to monitoring in return for permission to use company systems for personal use and the only consequence of withholding consent is that personal use is not permitted. German data protection authorities may not, however, consider that consent is freely given where consent is sought in the context of a specific and imminent investigation. And consent can be revoked by the employee. Absent consent, there is a risk that continuous, automated monitoring will be considered unreasonable unless there are legitimate suspicions of criminal activity or serious misconduct, or the monitoring is designed to mitigate serious risks to the company in the least intrusive way. For example, deploying monitoring tools to block the transmission of confidential or otherwise sensitive information in suspicious circumstances likely would be lawful. However, using monitoring tools to analyze employee behavior in order to assess whether employees might be inclined to engage in conduct that could harm the company will in most cases be viewed as disproportionate.

Additional Considerations. Prior to deployment, employers should assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Notably, such an assessment will be required under GDPR. Employers will want to confirm that they address other relevant data protection obligations, including

complying with appropriate employee requests to access, correct, or delete data, and data transfer restrictions.

Employers must obtain prior consent from works councils that may be established in the work place before engaging in monitoring that captures individual-level data regarding employees.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. Federal Data Protection Act; General Data Protection Regulation (effective May 25, 2018 along with the new Federal Data Protection Act); Telecommunications Act; German Criminal Code (Sections 201 and 206); Works Constitution Act.

Germany: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	4: *Works councils have a co-determination right regarding such monitoring and are often reluctant to consent to comprehensive monitoring. Coordinating with works councils can be time-consuming.*
Monitoring use of privileged access (e.g., administrator accounts)	3: *Estimate based on likelihood that little personal data will be involved (other than identifying the user) and heightened risks associated with administrative access.*
Monitoring use of applications	4: *Only if personal use is prohibited or if tools can monitor only the activities of individuals who have consented.*
Monitoring email communications	4: *If all personal use is prohibited or if individuals have consented to such monitoring.*
Monitoring employer-provided devices	4: *Need to establish justification for continuous monitoring given the likelihood of processing personal data in case personal use is prohibited.* *5: If personal use is allowed or at least tolerated.*
Monitoring Internet browsing	4: *Only if personal use is prohibited or if tools can monitor only the activities of individuals who have consented.*
Capturing on-screen activities	5: *Only if personal use is prohibited. Even when personal use is prohibited, such monitoring measures would most likely be considered to be inappropriate and unlawful.*
Keylogging	5: *Generally be considered unlawful by labor courts. In limited circumstances, may be allowed if personal use of resources is prohibited, the monitoring is strictly necessary for legitimate business purposes, and is prominently disclosed to employees.*
Monitoring behavior on social media and other channels	4: *Only where there are signs of misconduct and only on professional social media platforms. Monitoring of personal social media accounts will in most cases be considered to be inappropriate and unlawful.*
Monitoring employee-owned devices	5: *Estimate based on likely need to monitor only work activities. Personal activities likely cannot be monitored absent consent.*

ITALY

General considerations. Italian law imposes substantial restrictions on the monitoring of employee activities, including their use of information systems. As a general rule, Italian labor law prohibits employers from using technologies to investigate or monitor employees' activities. And sampling communications for manual review is generally prohibited. However, employers may deploy monitoring technologies as strictly necessary for the following, limited purposes: (1) achieving the employers' organizational or production needs; (2) workplace security; or (3) protecting company assets. For example, employers may use technologies that log metadata of electronic communications to maintain and operate communications tools; scan systems and networks to detect viruses or other malicious code; or block access to inappropriate online content. Employers may not use monitoring data for other purposes, nor may employers combine monitoring data with other data sets to monitor working activities. When deploying monitoring tools that could facilitate even limited, remote monitoring of employee activities, employers generally must enter into agreements with trade union representatives or obtain authorizations from the local employment office. There are limited exceptions to this requirement, such as where employers have legitimate suspicions of illicit activities and monitoring is conducted to identify misconduct and protect company assets.

Monitoring practices that involve the processing of personal data must collect, retain, and use personal data only as necessary to accomplish legitimate business purposes that are not outweighed by the adverse impact on employee privacy interests.

Employers may not record employees' attempts to access inappropriate web sites, and communications metadata may be retained only for up to seven days.

Employers may access and review emails and other communications only if they show signs of criminal activity or serious misconduct that would cause harm to the organization.

Notification Considerations	Consent Considerations
Employers must provide employees with clear notice about: (1) the types of personal data that may be collected; (2) the purposes of collection; (3) how the data will be used; (4) the retention of personal data; and (5) the recipients, if any, of the personal data. Employers must also provide clear information about acceptable use of resources and the consequences of misuse.	Consent does not serve as a reasonable justification for monitoring employee activities as there is a presumption that employees are not able to freely consent to demands from employers. Employers that implement monitoring tools in line with the restrictions noted above may engage in monitoring without obtaining consent.

Additional Considerations. Prior to deployment, employers should assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Notably, such an assessment will be required under GDPR.

Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access, correct, or delete data, and data transfer restrictions.

Official Guidance. Italian Data Protection Authority, 2007 Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context; Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. Data Protection Code; General Data Protection Regulation (effective May 25, 2018); Workers' Bill (no official English version).

Italy: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	4: *Monitoring metadata only for limited purposes.*
Monitoring use of privileged access (e.g., administrator accounts)	3: *Access logs of system administrators must be retained for six months. Due to identification of the employee activity, appropriate controls should be in place.*
Monitoring use of applications	4: *Monitoring metadata only for limited purposes.*
Monitoring email communications	4: *Monitoring metadata only for limited purposes.*
Monitoring employer-provided devices	4: *Metadata or scanning for malicious software only.*
Monitoring Internet browsing	5: *Only on an aggregate level and for limited purposes.*
Capturing on-screen activities	5: *Only for limited purposes.*
Keylogging	5: *Only for defensive controls*
Monitoring behavior on social media and other channels	4: *Only on the basis of a demonstrated legitimate interest of the controller and provided there are no other means to meet that specific purpose.*
Monitoring employee-owned devices	5: *Only on an aggregate level and for limited purposes.*

Employers may not record employees' attempts to access inappropriate web sites, and communications metadata may be retained only for up to seven days.

NETHERLANDS

General considerations. As in other EU Member States, monitoring that involves the processing of personal data must satisfy the test of reasonableness. Such monitoring is generally permitted if it is strictly necessary for a legitimate business purpose, if the adverse impact of monitoring on employees does not outweigh the legitimate purpose, if the nature and scope of monitoring is transparently disclosed to employees, and if monitoring is conducted in the least intrusive manner possible.

Assessing the reasonableness of monitoring is a highly fact-dependent exercise. Using automated monitoring tools that are designed to detect violations of law or regulations, to protect company systems and networks against malicious activities, or to prevent the disclosure of confidential or proprietary information generally will satisfy the test of proportionality. However, automatically monitoring communications that are clearly personal to identify violations of non-critical policies may be considered disproportionate. Sampling and manual review of communications is considered inherently more intrusive than the use of automated monitoring tools. Employers should confirm that the scope of monitoring is reasonable, that monitoring data is retained no longer than necessary (and for no longer than six months), and that access to monitoring data is limited.

If monitoring tools do not capture personal data, the tools are not subject to the restrictions of data protection law.

Employers are generally prohibited from accessing the contents of unopened electronic messages unless the sender and all intended recipients consent. Accessing unopened messages is permitted if done solely for the purpose of identifying business communications, such as opening messages to former employees to maintain business continuity.

Notification Considerations	Consent Considerations
Employers must provide notice to employees regarding monitoring that involves the processing of personal data unless there are legitimate suspicions of criminal misconduct or substantial malfeasance. Employees should have ready access to information about: (1) the types of personal data that will be collected; (2) when personal data will be collected; (3) the purposes of collection; (4) how the data will be used; (5) the retention of personal data; (6) transfers of data outside the EU; (7) the recipients, if any, of personal data; (8) their rights regarding personal data; and (9) contact information for entities processing the data.	Employee consent is not considered a valid consent under current Dutch law and may not be respected under GDPR.

Additional Considerations. Prior to deployment, employers should assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Notably, such an assessment will be required under GDPR or equivalent laws.

Employers must consult with works councils, if they have been established, prior to deploying monitoring programs. And employers may not monitor communications sent between works council members.

Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access or delete data, and data transfer restrictions.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. Dutch Data Protection Act; General Data Protection Regulation (effective May 25, 2018); Dutch Telecommunications Act; Universal Service and End User Interests Decree; Works Councils Act.

Employers should confirm that the scope of monitoring is reasonable, that monitoring data is retained no longer than necessary (and for no longer than six months), and that access to monitoring data is limited.

Netherlands: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	1: *Data protection impact assessment required if metadata is tied to specified individuals. Such monitoring likely has a reduced impact on employees.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	2: *Estimate based on monitoring of the types of applications used rather than the specific activities.*
Monitoring email communications	3: *Data protection impact assessment required.*
Monitoring employer-provided devices	3: *Data protection impact assessment required.*
Monitoring Internet browsing	4: *Data protection impact assessment required. Employers must consider whether goals can be achieved by blocking access to inappropriate sites without monitoring Internet use.*
Capturing on-screen activities	4: *Data protection impact assessment required. Presumption that monitoring has a more substantial adverse impact on employees.*
Keylogging	5: *Data protection impact assessment required. Such monitoring will be considered reasonable only in exceptional circumstances (e.g., legitimate suspicions of criminal activity).*
Monitoring behavior on social media and other channels	5: *Data protection impact assessment required. Such monitoring will be considered reasonable only in exceptional circumstances (e.g., legitimate suspicions of criminal activity).*
Monitoring employee-owned devices	4: *Estimate based on likely need for separation of work and personal environments for monitoring and wiping. Employees generally have a right to be able to shield private communications from work-related monitoring.*

SPAIN

General considerations. As in other European Union Member States, monitoring that involves the processing of personal data must satisfy the test of reasonableness. This test involves determining whether monitoring effectively achieves a reasonable business purpose (e.g., detecting and preventing criminal activity or similarly serious misconduct) in the least intrusive way without being outweighed by the impact on employees' privacy. Sampling communications or records of employee activities generally will be viewed as being more intrusive than the use of automated monitoring tools. Automated tools that focus on preventing, rather than detecting, misuse are preferred.

Employers should provide employees with clear notices that limit any expectations of confidentiality or privacy that employees may have regarding their use of communications resources.

If monitoring tools do not capture personal data, the tools are not subject to the requirements under data protection law.

Notification Considerations	Consent Considerations
Employers must provide employees with a policy regarding the use of information technologies that informs employees about: (1) the types of personal data that may be collected; (2) the purposes of collection; (3) how the data will be used; (4) the retention of personal data; (5) international transfers of data; (6) the recipients, if any, of personal data; (7) the identity and address of the entity that controls the data processing activities; (8) whether providing the data is mandatory and the consequences of withholding data; and (9) how employees may exercise their rights regarding personal data. The policy also should inform employees that communication systems should not be used for private or personal purposes; that employees should have no expectation of privacy with respect to their use of communications systems; and that employers may periodically review, access, inspect, monitor, or process communications without further notice.	Except in very limited circumstances, consent does not serve as a lawful basis for the processing of employees' personal data because of the presumption that employees cannot freely give their consent. Employers that implement monitoring tools in the manner described above may engage in monitoring without obtaining consent.

Additional Considerations. Prior to deployment, employers should assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Notably, such an assessment will be required under GDPR. Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access, correct, or delete data, and data transfer restrictions.

Employers should avoid capturing personal data that is inadequate, irrelevant, or excessive, as well as employees' sensitive data (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history), unless there is a legal obligation or employees have consented to the processing of such sensitive information. Employers relying on consent should confirm that such consent will be viewed as freely given.

Automated tools that focus on preventing, rather than detecting, misuse are preferred.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. Data Protection Act 15/1999; Royal Decree Relating to Personal Data Protection 1720/2007; General Data Protection Regulation (effective May 25, 2018); Article 18.3 of the Spanish Constitution (Spanish); Spanish Workers Statute (Spanish).

Spain: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	2: *Metadata only. So, impact is reduced.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	2: *Metadata only. So, impact is reduced.*
Monitoring email communications	3: *Conduct data protection impact assessment and provide clear notice.*
Monitoring employer-provided devices	3: *Conduct data protection impact assessment and provide clear notice.*
Monitoring Internet browsing	4: *Conduct data protection impact assessment and provide clear notice. Presumption of higher expectation of privacy.*
Capturing on-screen activities	4: C*onduct data protection impact assessment and provide clear notice. Presumption of higher expectation of privacy.*
Keylogging	4: *Conduct data protection impact assessment and provide clear notice. Presumption of higher expectation of privacy.*
Monitoring behavior on social media and other channels	4: *Conduct data protection impact assessment and provide clear notice. Presumption of higher expectation of privacy.*
Monitoring employee-owned devices	5: *Conduct data protection impact assessment and provide clear notice. Employee consent likely required as the expectation of privacy with regard to employee-owned devices likely outweighs employers' interests. Separate work and personal aspects of device activity/storage.*

SWEDEN

General considerations. Monitoring that involves the processing of personal data must have a legal basis. The legal ground employers generally rely on is to achieve the employer's legitimate interests on the basis of a general balancing of interests. In a limited range of circumstances, monitoring might be grounded on the necessity to satisfy a contract between the employer and the employee; however, this is the exception. On the grounds of legitimate interests, monitoring is generally permitted if it is strictly necessary for a legitimate business purpose, if the adverse impact of monitoring on employees does not outweigh the purposes of the monitoring, if the nature and scope of monitoring is transparently disclosed to employees, and if monitoring is conducted in the least intrusive manner possible. Under current law, legitimate business purposes include promoting the employer's commercial interests as well as detecting and preventing criminal activity or similarly serious misconduct. However, commercial interests alone likely will not support continuous monitoring of employee activities, as the impact on employees would be disproportionate. Sampling communications or records of employee activities generally will be viewed as being more intrusive than the use of automated monitoring tools.

Employers should access personal communications and files only in exceptional circumstances, such as where there are substantial suspicions of criminal activity or similarly serious misconduct.

If monitoring tools do not capture personal data, the tools are not subject to the restrictions of data protection law.

Notification Considerations	Consent Considerations
Employers must provide notice to employees regarding monitoring that involves the processing of personal data unless there are strong suspicions of criminal misconduct or substantial malfeasance. Employees should have ready access to information about: (1) the types of personal data that may be collected; (2) why the personal data is collected; (3) how the personal data will be used; (4) how long the personal data will be retained; (5) the potential recipients of the personal data; (6) information about any transfer of personal data to countries outside of the EU; (7) the employees' right to request access, rectification, and erasure of personal data; and (8) how to contact the data processor.	Consent is not required if monitoring is conducted on the grounds described above. Consent is not a reliable basis for monitoring as employee's consent must be given freely, which is difficult to establish in employment contexts. Employee monitoring programs generally rely on the employer's legitimate interests, rather than consent, as a legal basis for processing.

Additional Considerations. Prior to deployment, employers should assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access, correct, or delete data, and data transfer restrictions.

Employers should avoid capturing employees' sensitive data information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history) unless there is a legal obligation to process the information or if it is necessary to protect certain vital interests. Employers may not store personal data regarding employees' criminal history.

Personal data may not be stored longer than is necessary to fulfill the legitimate purposes of the processing. The Swedish Data Inspection Board has advised that personal data should generally be held for no longer than three months and that employers should not store the personal data of employees after their employment ceases, unless there is a demonstrated need. If the employer is bound by a collective bargaining agreement with a trade union, the employer likely must consult with the trade union prior to introducing a monitoring scheme.

Official Guidance. Swedish Data Protection Board, Monitoring in Working Life; Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. Personal Data Act (official summary); General Data Protection Regulation (effective May 25, 2018); Co-Determination in the Workplace Act (no official English version).

Sweden: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	2: *Estimate based on limited personal data.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	2: *Estimate based on monitoring of the types of applications used rather than the specific activities. Perhaps a lower degree of effort is appropriate given likelihood that little personal data is involved.*
Monitoring email communications	3: *Data protection impact assessment required.*
Monitoring employer-provided devices	3: *Data protection impact assessment required.*
Monitoring Internet browsing	3: *Data protection impact assessment required.*
Capturing on-screen activities	4: *Data protection impact assessment with more substantial impact on employees.*
Keylogging	4: *Data protection impact assessment with more substantial impact on employees.*
Monitoring behavior on social media and other channels	4: *Data protection impact assessment with more substantial impact on employees.*
Monitoring employee-owned devices	5: *Estimate based on likely need for separation of work and personal environments for monitoring and wiping. There is a heighted risk of impact on employees' privacy rights.*

SWITZERLAND

General considerations. Employers are generally prohibited from monitoring employees' activities in ways that allow for the identification of employees. However, employers may use automated tools to continuously monitor employee activities if the monitoring does not readily identify particular employees (e.g., the monitoring collects only metadata or produces only aggregate reports). If an employer has reasonable suspicions of criminal activity or serious misconduct, the employer may engage in monitoring that enables the identification of employees but only if such monitoring is the least intrusive means to achieve the employer's goals. Automated and anonymous monitoring tools are therefore preferable to manual sampling techniques, which are likely to identify employees.

Notification Considerations	Consent Considerations
Employers must provide notice to employees regarding monitoring that involves the processing of personal data. Employees should have ready access to information about: (1) when information will be collected, (2) the purposes of collection, (3) how the information will be used, (4) the retention of information, and (5) the recipients, if any, of the information.	Consent generally may not serve as a lawful basis for monitoring employee activities due to the perception that employees cannot give their consent freely. Thus, employers will rely on other justifications for monitoring practices. Consent is required, however, for employers to review personal, rather than business, communications. Such consent must be specific to a particular situation and cannot be obtained in a general manner (e.g., via an employment agreement).

Additional Considerations. Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access or delete data and addressing restrictions on data sharing and crossborder data transfers.

Depending on any revisions to the Federal Data Protection Act that may be adopted in light of the GDPR, employers may need to conduct data protection impact assessments prior to deploying new monitoring programs or tools.

Official Guidance. Federal Data Protection and Information Commissioner, Spyware in the Workplace; Workplace Surveillance

Notable Laws or Regulations. Federal Data Protection Act (which may be modified to align with the General Data Protection Regulation); Ordinance to the Federal Data Protection Act; Swiss Criminal Code; Telecommunications Act (currently under revision); Ordinance on Telecommunication Services (currently under revision); Swiss Code of Obligations; Federal Act on Labor in Industry, Commerce and Trade (German); Ordinance 3 of the Labor Code (German).

Switzerland: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	2: *Ensure that monitoring is anonymous.*
Monitoring use of privileged access (e.g., administrator accounts)	3: *Estimate based on assessment that the increased risks associated with privileged access justify the monitoring of the use of privileged access.*
Monitoring use of applications	4: *Must be anonymous absent signs of misconduct.*
Monitoring email communications	4: *Must be anonymous absent signs of misconduct.*
Monitoring employer-provided devices	4: *Must be anonymous absent signs of misconduct.*
Monitoring Internet browsing	4: *Must be anonymous absent signs of misconduct.*
Capturing on-screen activities	5: *Permitted in exceptional circumstances that are disclosed in acceptable use policy.*
Keylogging	5: *Prohibited if continuously monitoring the employees activities.*
Monitoring behavior on social media and other channels	5: *Likely prohibited but for exceptional circumstances.*
Monitoring employee-owned devices	4: *Estimate based on likely need for separation of work and personal environments for monitoring and wiping.*

UNITED KINGDOM

General considerations. As in other EU Member States, monitoring that involves the processing of personal data must satisfy the test of reasonableness. Such monitoring is generally permitted if it is strictly necessary for a legitimate business purpose, if the adverse impact of monitoring on employees does not outweigh the legitimate purpose, if the nature and scope of monitoring is transparently disclosed to employees, and if monitoring is conducted in the least intrusive manner possible.

Assessing the reasonableness of monitoring is a highly fact-dependent exercise. Legitimate purposes for monitoring include detecting or preventing violations of law, regulations, or important internal policies. Monitoring the use of employer-provided systems to detect signs of serious misconduct or to prevent the disclosure of confidential or proprietary information may be proportional to the potential impact on employees. But monitoring communications that are clearly personal to identify violations of non-critical policies is likely to be considered disproportionate. Manual sampling records of employee conduct will generally be viewed as having a greater adverse impact than analyzing activities via automated tools. And preventing misuse in a manner that does not involve recording individual employees' activities is viewed as having less of an adverse impact on employees than does recording employee activities to detect signs of misuse. Accessing communications that are clearly personal in nature likely is unlawful absent legitimate suspicions of criminal activity, even where private use of work systems is expressly prohibited. These considerations apply to all individuals that employers engage for business purposes not just contracted employees.

Monitoring that involves the processing of sensitive information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history) likely will be lawful only if it is necessary to comply with a legal obligation.

If monitoring tools do not capture personal data, the tools are not subject to the restrictions of data protection law.

Monitoring that involves the interception of communications during transmission, is governed by the Regulation of Investigatory Powers Act. Such access is permitted if both the sender and recipient consent or if the access involves analyzing business-related communications for the purpose of monitoring compliance with United Kingdom laws and regulations or reasonable internal policies.

Notification Considerations	Consent Considerations
Employers must provide notice to employees regarding monitoring that involves the processing of personal data unless there are legitimate suspicions of criminal misconduct or substantial malfeasance. Employees should have ready access to information about: (1) when personal data will be collected; (2) the purposes of collection; (3) how the data will be used; (4) the retention of personal data; and (5) the recipients, if any, of the data.	Consent is not required if monitoring is conducted on the basis of employers' legitimate interests described above. Consent might justify monitoring that goes beyond what is reasonably necessary to accomplish legitimate business purposes, but this is not a favored practice and may not be respected under the GDPR. Consent must be freely given, which is difficult to establish in the employment context. And employees would have the right to withdraw consent, thereby suspending monitoring where consent is the only legal basis for the activity. Employee monitoring programs generally rely on the employer's legitimate interests, rather than consent, as a legal basis.

Additional Considerations. Prior to deployment, employers should assess insider threat programs to confirm that the legitimate objectives of the programs are not outweighed by the potential adverse impact on employees. Notably, such assessments will be required under GDPR and equivalent laws. Steps should be taken to balance the legitimate interests of the employer and the fundamental rights and freedoms of employees.

Monitoring that involves the processing of sensitive information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history) likely will be lawful only if it is necessary to comply with a legal obligation.

Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access or delete data and data transfer restrictions.

Official Guidance. The Information Commissioner's Office, Employment Practices Code and Supplementary Guidance on the Employment Practices Code; Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws and Regulations. Data Protection Directive 95/46/EC; Data Protection Act 1998; General Data Protection Regulation (effective May 25, 2018) or equivalent; Regulation of Investigatory Powers Act 2000 (addressing interceptions of communications); Telecommunications (Lawful Business Practice) Regulation 2000 (addressing interceptions of communications).

United Kingdom: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	1: *Data protection impact assessment required if metadata is tied to specified individuals. Such monitoring likely has a reduced impact on employees.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Estimate based on likelihood that little personal data will be involved. Moreover, due to heightened risks associated with administrative access, employees have a low expectation of privacy in this context.*
Monitoring use of applications	2: *Estimate based on monitoring of the types of applications used rather than the specific activities. Perhaps a lower degree of effort is appropriate given likelihood that little personal data is involved.*
Monitoring email communications	3: *Data protection impact assessment required.*
Monitoring employer-provided devices	3: *Data protection impact assessment required.*
Monitoring Internet browsing	4: *Data protection impact assessment required. Employers must consider whether goals can be achieved by blocking access to inappropriate sites without monitoring Internet use.*
Capturing on-screen activities	3: *Data protection impact assessment required. Such monitoring is presumed to have a more substantial adverse impact.*
Keylogging	5: *Data protection impact assessment required. Such monitoring will be considered reasonable only in exceptional circumstances (e.g., legitimate suspicions of criminal activity).*
Monitoring behavior on social media and other channels	5: *Data protection impact assessment required. Such monitoring will be considered reasonable only in exceptional circumstances (e.g., legitimate suspicions of criminal activity).*
Monitoring employee-owned devices	4: *Estimate based on likely need to separate work and personal environments for monitoring and wiping. Employees generally have a right to be able to shield private communications from work-related monitoring.*

AUSTRALIA

General considerations. Automated monitoring and manual sampling of employee use of email, instant messaging, and other electronic communications tools is generally permitted under federal, state, and territorial statutes. The Privacy Act generally supports the use and disclosure of information collected via monitoring activities when an employer has reason to suspect that an employee has engaged in unlawful activities or otherwise serious misconduct.

In New South Wales, Victoria, and the Australian Capital Territory, employers must obtain express consent to monitor employee activities on devices or resources that are not provided by or at the expense of the employer when the employee is not at the employer's workplace or is not otherwise conducting work for the employer.

Federal law permits employers to intercept communications while in transit provided that employers inform individuals making the communications or the communications are intercepted for network protection purposes as authorized in writing by the person responsible for the employer's network.

Notification Considerations	Consent Considerations
Employers should provide employees with transparent monitoring notices that describe monitoring activities and explain the purposes for which monitoring is conducted. In New South Wales and the Australian Capital Territory, such notice must be provided at least fourteen days prior to implementing monitoring programs. Prospective employees must receive the notice before they start work. Such notice must be delivered in such a way that it is reasonable to assume that employees are aware of the employer's monitoring policies. The notice must indicate: (1) the kind of surveillance to be carried out (e.g., camera, computer, or tracking); (2)how the surveillance will be carried out; (3) when the surveillance will start; (4) whether the surveillance will be continued or intermittent; and (5) whether surveillance will be ongoing or conducted for a limited period.	Express consent generally is not required to monitor employees' use of computers and information technologies in the workplace. Consent can authorize otherwise prohibited monitoring activities, such as monitoring of employee-provided devices and of employees' activities outside the workplace.

Additional considerations. Employers will want to confirm that they treat information in accordance with the Australian Privacy Principles, including securing information, addressing cross-border data transfers, and responding to employee requests to access personal information acquired in the course of monitoring.

Official Guidance. Fair Work Ombudsman, Workplace Privacy Best Practice Guide; Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines.

Notable Laws or Regulations. Privacy Act 1988; Telecommunications (Interception and Access) Act; Workplace Surveillance Act (New South Wales); Workplace Privacy Act (Australian Capital Territory).

Australia: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	1: *Little personal data involved.*
Monitoring use of privileged access (e.g., administrator accounts)	1: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	1: *Estimate based on monitoring of the types of applications used rather than the specific activities.*
Monitoring email communications	2: *Notice required. Consider limiting to network protection purposes.*
Monitoring employer-provided devices	2: *Notice required.*
Monitoring Internet browsing	2: *Notice required. Consider limiting to network protection purposes.*
Capturing on-screen activities	2: *Notice required.*
Keylogging	2: *Notice required.*
Monitoring behavior on social media and other channels	4: *Express consent due to "at work" considerations in certain jurisdictions.*
Monitoring employee-owned devices	4: *Need express consent in certain jurisdictions.*

CANADA

General Considerations. Employee monitoring is governed by federal and provincial privacy laws, which focus on the reasonableness of monitoring. Under federal law, employers may engage in monitoring that involves the processing of personal information if the monitoring is necessary to satisfy an objective of the employer, the monitoring is likely to accomplish the objective, the impact on employee privacy is proportional to the benefits gained by the employer, and there is no less intrusive means of accomplishing the objective.

Provincial laws follow a substantially similar test, with some provinces considering the sensitivity and volume of data collected and whether employers have engaged in reasonable assessments of the impact and benefits of the monitoring. Regardless of the test use, the conclusion of the reasonableness assessment generally is the same.

Automated monitoring of employee use of communications tools generally is viewed as less intrusive than random sampling.

Notification Considerations	Consent Considerations
Providing notice to employees generally bolsters arguments that monitoring is reasonable, as notices minimize employees' expectations of privacy. Notices should provide employees with transparent information about: (1) the nature of personal information collected and (2) the purposes for which the information will be used and disclosed. Employers may wish to notify employees that they should have no expectation of privacy when using company resources. If providing notice to an employee would defeat the purposes of monitoring (e.g., when a targeted investigation is underway), monitoring without notice may be permitted.	In most cases, express consent is not required if employers provide notice of the collection and use of personal information and the monitoring is reasonable in light of the employment relationship. However, employers are required to obtain express consent from employees prior to installing computer programs on employee-owned devices.

Additional Considerations. Employers will want to confirm that provincial data transfer requirements are satisfied.

Automated monitoring is viewed as less intrusive and more reasonable than random sampling of employee communications. Thus, automated monitoring systems are more likely to be permissible than equivalent manual systems. Personal information flagged for manual review should be used only for the disclosed purposes and not general disciplinary purposes. If a computer program will be installed on an employee's computer that is owned by the employee, express consent must be obtained pursuant to Canada's Anti-Spam Legislation.

Official Guidance. Office of the Privacy Commissioner of Canada, Privacy in the Workplace; Office of the Information and Privacy Commissioner for BC, IT Security and Employee Privacy: Tips and Guidance.

Notable Laws or Regulations. Personal Information Protection and Electronic Documents Act; An Act Respecting the Protection of Personal Information in the Private Sector (Quebec); Personal Information Protection Act (Alberta); Personal Information Protection Act (British Columbia); Anti-Spam Legislation.

Employers should avoid capturing employees' sensitive data information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, or criminal history) unless there is a legal obligation to process the information.

Canada: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	1: *Unlikely to raise significant privacy issues.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	2: *Estimate based on monitoring of the types of applications used rather than the specific activities. Perhaps a lower degree of effort is appropriate given likelihood that little personal data is involved.*
Monitoring email communications	3: *Assess reasonableness and provide notice.*
Monitoring employer-provided devices	3: *Assess reasonableness and provide notice.*
Monitoring Internet browsing	3: *Assess reasonableness and provide notice.*
Capturing on-screen activities	4: *Reasonableness may be difficult to establish.*
Keylogging	4: *Reasonableness may be difficult to establish.*
Monitoring behavior on social media and other channels	4: *Reasonableness may be difficult to establish.*
Monitoring employee-owned devices	4: *Estimate based on likely need to separate work and personal environments for monitoring and wiping. May need to obtain express consent for installation of software.*

SINGAPORE

General considerations. Although consent is generally required for the collection, use, and disclosure of personal data, employers may process personal data without consent to support monitoring programs if such processing reasonably supports the management or termination of employment relationships, including as necessary to evaluate the suitability, eligibility, or qualifications of an employee for promotion or continued employment.

To assess the reasonableness of monitoring, employers must consider whether a reasonable person would consider the monitoring appropriate in the circumstances. If monitoring captures more information than is necessary to manage or terminate employment relationships, consent likely is required. Using automated tools to flag activities for review only when there are signs of misconduct likely will be considered more reasonable than sampling employee activities for manual review.

Notification Considerations	Consent Considerations
Employers generally must provide employees with transparent notices about: (1) the types of personal data that may be collected and (2) the purposes for which it will be used. However, employers need not inform employees about the collection and use of personal data solely for purposes of evaluating the suitability, eligibility, or qualifications of an employee for promotion or continued employment. Employers must, upon request, provide employees with the contact information of someone able to discuss questions about the employer's collection, use, and disclosure of personal data.	Employers need not obtain consent for monitoring activities that reasonably support the management or termination of employment relationships, including activities that are necessary to evaluate the suitability, eligibility, or qualifications of an employee for promotion or continued employment or for evaluation purposes.

Additional Considerations. Employers will want to confirm that they address other relevant data protection obligations, including securing any personal data collected; taking reasonable steps to confirm that personal data is accurate and complete, particularly if the personal data is likely to be used to make a decision that affects the employee or if the personal data will be disclosed to a third party for their own use; deleting personal data when it is no longer needed; complying with appropriate employee requests to access or correct data; and addressing data transfer obligations.

Official Guidance. Personal Data Protection Commission, Advisory Guidelines on the Personal data Protection Act for Selected Topics (Section 5).

Notable Laws or Regulations. Personal Data Protection Act 2012 (No. 26 of 2012).

Singapore: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	2: *Confirm reasonableness.*
Monitoring use of privileged access (e.g., administrator accounts)	1: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	1: *Estimate based on monitoring of the types of applications used rather than the specific activities. Perhaps a lower degree of effort is appropriate given likelihood that little personal data is involved.*
Monitoring email communications	2: *Confirm reasonableness.*
Monitoring employer-provided devices	2: *Confirm reasonableness.*
Monitoring Internet browsing	2: *Confirm reasonableness.*
Capturing on-screen activities	4: *Increased level of effort due to need to demonstrate reasonableness.*
Keylogging	4: *Increased level of effort due to need to demonstrate reasonableness.*
Monitoring behavior on social media and other channels	4: *Increased level of effort due to need to avoid unreasonable collection of personal data that is likely to be found on social media and other channels.* 2: *If monitoring only publicly-available information.*
Monitoring employee-owned devices	4: *If corporate data is in employee-owned devices, increased level of effort due to need to avoid unreasonable monitoring of personal activities/items and to get explicit consent from the employee.* 5: *If the employee-owned devices are used solely for personal activities, it would be difficult to justify that such monitoring is reasonable for managing or terminating that employee relationship or for evaluation purposes.*

SOUTH AFRICA

General considerations. Employers' monitoring activities are primarily governed by the Regulation of the Interception of Communications and Provisions of Communication-Related Information Act ("RICA"), which covers interceptions of electronic communications via a broad range of monitoring devices, including keyloggers and screen capture technologies.

RICA permits employers to monitor and record facts related to employees' work-related activities or activities conducted using employer-provided communications systems provided that: (1) employers undertake all reasonable efforts to obtain express consent from employees or provide employees with advance notice of the monitoring; (2) the chief executive officer, or equivalent officer of the organization, consents to the monitoring; and (3) the monitoring is conducted solely for purposes of investigating or detecting unauthorized use of communications systems, securing the operation of communications systems, or establishing the existence of any facts related to the employer's business interests.

Some advocates have argued that RICA permits employers to monitor employee activities for any purposes provided that employees consent to the monitoring. However, the predominant interpretation of RICA is that consent authorizes monitoring activities only to the extent that they are conducted for the purposes described above.

When South Africa's data protection law, the Protection of Personal Information Act ("POPIA"), takes full effect it may establish notification requirements, which are discussed below.

Notification Considerations	Consent Considerations
If relying on notice to authorize monitoring, employers must take all reasonable efforts to provide employees with notice that their use of and activities associated with communications systems may be monitored. When POPIA takes full effect, and subject to any regulations that may be issued, employers may need to provide employees with clear notices about: (1) the types of personal information that will be collected; (2) the purposes of collection; (3) whether employees are required to provide personal information; (4) the consequences of not providing personal information; (5) the laws authorizing or requiring the collection; (6) the recipients, if any, of the information; (7) contact information for the entity processing the information; and (8) their rights regarding personal information. Additional disclosures may be required.	Employee consent can authorize monitoring activities subject to the restrictions noted above, provided that the consent is voluntary, specific, and informed. Employees can withdraw consent on reasonable grounds at any time. So, employers may wish to rely on notice rather than consent to authorize monitoring.

Additional Considerations. Employers will want to confirm that they address other relevant data protection obligations, including complying with data security obligations and data transfer restrictions.

Notable Laws or Regulations. The Constitution of the Republic of South Africa; Regulation of the Interception of Communications and Provision of Communication-Related Information Act; Protection of Personal Information Act.

South Africa: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	2: *Notice or consent.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Notice or consent.*
Monitoring use of applications	2: *Notice or consent.*
Monitoring email communications	2: *Notice or consent.*
Monitoring employer-provided devices	2: *Notice or consent.*
Monitoring Internet browsing	2: *Notice or consent.*
Capturing on-screen activities	2: *Notice or consent.*
Keylogging	2: *Notice or consent.*
Monitoring behavior on social media and other channels	4: *POPIA may limit processing here based on legitimate interests.*
Monitoring employee-owned devices	4: *Confirm that interceptions align with RICA given use of personal device.*

RICA permits employers to monitor and record facts related to employees' work-related activities or activities conducted using employer-provided communications systems provided that: (1) employers undertake all reasonable efforts to obtain express consent from employees or provide employees with advance notice of the monitoring; (2) the chief executive officer, or equivalent officer of the organization, consents to the monitoring; and (3) the monitoring is conducted solely for purposes of investigating or detecting unauthorized use of communications systems, securing the operation of communications systems, or establishing the existence of any facts related to the employer's business interests.

TURKEY

General considerations. Employee monitoring activities are governed by Turkish data protection law, which is largely based on the principles set forth in the EU's Data Protection Directive 95/46/EC; rulings from the Court of Appeal precedents; and Labor Code No. 4847. Employers may engage in monitoring activities that involve the processing of personal data if employees provide express consent, if the activities are required by law, or if the activities support employers' legitimate interests that are not outweighed by employee privacy interests. Using automated tools to monitor employee activities, rather than engaging in manual sampling, and monitoring metadata rather than contents of communications are examples of practices that may effectively support employers' objectives while reducing the impact on employees.

Employers must obtain employees' express consent for monitoring activities that involve the processing of sensitive personal data, such as data relating to race, ethnic origin, political opinions, religion, philosophical beliefs, membership in an association, foundation, or trade union, health, sexual orientation, criminal history, biometrics, or genetics.

Notification Considerations	Consent Considerations
Employers must provide employees with clear notice about: (1) the types of personal data that will be collected; (2) when personal data will be collected; (3) the purposes of collection; (4) how the data will be used; (5) the identity of the entity that controls the processing of the data; (6) the recipients, if any, of personal data; and (7) rights regarding their personal data.	Express consent is required for monitoring activities that involve the processing of sensitive personal data. Employers may wish to rely on consent for monitoring as monitoring Internet use or use of communications tools may capture sensitive personal data. Where monitoring does not involve the processing of sensitive personal data, employers may rely on their legitimate interests as a legal basis for monitoring.

Additional Considerations. Employers will want to confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access, correct, or delete data, cross-border data transfer restrictions, data security obligations, and registration requirements.

Notable Laws or Regulations. Law on the Protection of Personal Data; Labor Code No. 4857.

Turkey: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	1: *Limited impact on privacy.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	2: *Estimate based on monitoring of the types of applications used rather than the specific activities. Perhaps a lower degree of effort is appropriate given likelihood that little personal data is involved.*
Monitoring email communications	3: *Confirm proportionality.*
Monitoring employer-provided devices	3: *Confirm proportionality.*
Monitoring Internet browsing	3: *Confirm proportionality.*
Capturing on-screen activities	4: *May be considered to have a substantial impact on employees.*
Keylogging	4: *May be considered to have a substantial impact on employees.*
Monitoring behavior on social media and other channels	4: *May be considered to have a substantial impact on employees.*
Monitoring employee-owned devices	4: *Estimate based on likely need to separate work and personal environments for monitoring and wiping.*

UNITED STATES

General considerations. In the United States, employee monitoring activities are governed by a range of federal and state laws providing protections for electronic communications. For example, some states require employers to provide employees with written notice of monitoring activities. However, the federal Cybersecurity Information Sharing Act of 2015 ("CISA") provides a broad immunity for employee monitoring activities undertaken for cybersecurity purposes.

Insider threat monitoring programs that are conducted for "cybersecurity purposes" are permitted under CISA. A cybersecurity purpose is a purpose aimed at "protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." A cybersecurity threat is an action not protected by the First Amendment to the Constitution of the United States that is conducted "on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system." A security vulnerability is "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control."

Given the breadth of CISA's definitions and protections from liability, insider threat monitoring programs that are conducted for legitimate business purposes focused on securing information systems, or the information stored on them, likely will be lawful in the United States.

Notification Considerations	Consent Considerations
CISA does not impose notice requirements. However, providing employees with notice of monitoring activities is a leading practice and can mitigate the risks of employee complaints and reduced moral if monitoring activities become known in the workforce. Providing transparent notice will also mitigate risk in the event that a court interprets CISA to not provide immunity for failure to provide notice as required under state laws or if a court rules that aspects of an insider threat program are not conducted for a cybersecurity purpose. Such notice should provide employees with: (1) clear information about the types of activities and (2) communications the employer monitors.	CISA does not impose consent requirements. However, as discussed in the notification cell, providing transparent notice of monitoring may mitigate certain risks. And such notice, if clearly presented to employees, can serve to establish employee consent to the monitoring of communications under federal and state laws.

Additional Considerations. Although CISA's protections against liability are broad, CISA does not establish an unfettered right to deploy monitoring programs. Employers should confirm with counsel that programs are conducted for cybersecurity purposes as defined under CISA. To the extent that activities may be viewed as going beyond cybersecurity purposes, employers should confirm that the activities comply with applicable federal and state laws, which may include federal and state eavesdropping and wiretap laws, as well as state laws requiring employers to notify employees.

Notable Laws or Regulations. Cybersecurity Information Sharing Act (liability protection language).

United States: Estimated Level of Effort for Employee Monitoring Activities

The chart below reflects the estimated level of effort needed to lawfully implement specific types of employee monitoring activities. The level of effort is assessed on a scale of 1 to 5, with 1 reflecting an estimate that employers may implement the monitoring with a minimal amount of effort, and 5 reflecting that the activity is generally prohibited or requires a substantial amount of compliance resources to implement in accordance with applicable laws.

Monitoring temporal metadata (e.g., logon, logoff, session length)	1: *Confirm that monitoring is for a cybersecurity purpose. Metadata is less sensitive.*
Monitoring use of privileged access (e.g., administrator accounts)	1: *Confirm that monitoring is for a cybersecurity purpose. Greater presumption that monitoring of privileged access addresses such a purpose.*
Monitoring use of applications	2: *Confirm that monitoring is for a cybersecurity purpose.*
Monitoring email communications	2: *Confirm that monitoring is for a cybersecurity purpose.*
Monitoring employer-provided devices	2: *Confirm that monitoring is for a cybersecurity purpose.*
Monitoring Internet browsing	2: *Confirm that monitoring is for a cybersecurity purpose.*
Capturing on-screen activities	2: *Confirm that monitoring is for a cybersecurity purpose.*
Keylogging	2: *Confirm that monitoring is for a cybersecurity purpose.*
Monitoring behavior on social media and other channels	3: *Confirm that monitoring is for a cybersecurity purpose. There is potential for such monitoring to extend beyond what some might consider a cybersecurity purpose.*
Monitoring activities on employee-owned devices	3: *Avoid monitoring clearly personal activities or confirm that such monitoring addresses a cybersecurity purpose.*

Given the breadth of CISA's definitions and protections from liability, insider threat monitoring programs that are conducted for legitimate business purposes focused on securing information systems, or the information stored on them, likely will be lawful in the United States.

About the Authors

Harriet Pearson
Partner, Washington, D.C and New York
Clients value Harriet Pearson's extensive experience in every aspect of cybersecurity & privacy law, policy, and compliance. Drawing on her in-house experience as IBM's first and longstanding global chief privacy officer and security counsel, since joining Hogan Lovells in 2012, Harriet has been advising companies and boards on cyber and data risk governance, global regulatory compliance, and breach investigations and enforcement. She is Chambers-ranked and was named: North America's "Legal Innovator of the Year" by the Financial Times in both 2015 and 2016; a "Cybersecurity and Privacy Trailblazer" by the National Law Journal; and one of the 500 "Leading Lawyers in America" by LawDragon. Harriet leads the firm's global multi-disciplinary Cybersecurity Solutions team.

W. James Denvil
Senior Associate, Washington, D.C.
James Denvil has a passion for helping companies navigate the complex challenges associated with deploying and managing today's information technologies and systems. He understands that one of the most important elements of client service is listening, and once he understands a client's needs, he leverages his analytical training to identify potential issues, dissect alternative approaches, and deliver practical solutions. James regularly advises clients on a range of technology issues, including developing products and services for the Internet of Things, implementing Big Data technologies, incident response, global data transfers, privacy risk assessments and mitigation, recurring payments, and employee monitoring.

The authors would like to acknowledge and thank Forcepoint for their support. Special thanks to John D. Holmes, Fritz Fielding, Marlene Connolly, and Neil Thacker

,

About Hogan Lovells Privacy and Cybersecurity Practice

The Hogan Lovells Privacy and Cybersecurity team has specialized in privacy, data protection, and cybersecurity for over 25 years. Today, Hogan Lovells has one of the largest and most experienced Privacy and Cybersecurity practices in the world, with teams spanning Europe, the United States, and Asia. We are at the pinnacle of privacy practices in the United States as reflected by our receipt of the prestigious Chambers USA Privacy and Data Security Team of the Year in 2015 and 2017. Moreover, with over 80 lawyers focused on privacy and cybersecurity worldwide, our team has a deep understanding of the issues facing all industries and a pulse on global privacy trends. For jurisdictions where we do not have a physical presence, we have a trusted and well-established network of local connections, meaning we can provide practical legal solutions wherever your work takes you. We assist clients with all of their compliance and risk management challenges, drafting policies and providing advice on legal issues and strategic governance. We also play an important role in the development of public policy regarding the future regulation of privacy and data protection. We provide the latest privacy and data protection legal developments and trends to our clients via our blog, Chronicle of Data Protection.

About the Sponsor: Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance.

Regardless of how attacks originate, they ultimately inflict the most damage at the points in which people interact with critical business data and intellectual property. These 'human points' of interaction have the potential to undermine even the most comprehensively-designed systems in a single malicious or unintentional act.

We offer a systems-oriented approach to insider threat detection and analytics, cloud-based user and application protection, next-gen network protection, data security and systems visibility. As technology and users' needs evolve, we are constantly looking to expand our offerings while staying true to our core in protecting the human point.

Only by understanding the intent behind a user's actions can we recognize the difference between good and bad cyber behaviors. It's Forcepoint's goal not just to recognize that difference, but to provide intelligent systems that allow good employee behavior and facilitate business while stopping bad cyber behaviors.

For more about Forcepoint, visit www.Forcepoint.com.