Hogan Lovells

Protecting the Workforce and Information in a Global Landscape: A Legal Review

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

Sponsored by:
Forcepoint

Protecting the Workforce and Information in a Global Landscape:
A Legal Review
by

Harriet Pearson, Washington, DC & New York
James Denvil, Washington, DC[1]

Executive Summary

Organizations around the world face substantial and increasing cybersecurity-related threats to operations, reputation, and the bottom line. Cyber risk profiles are changing, particularly in light of the increase in agile working arrangements driven by the COVID-19 pandemic and other factors. Organizations may have confidence that the only users remotely accessing information resources are doing so with authorized credentials, but they may not know who is using those credentials or whether authorized users are engaged in unauthorized activities. As a result, organizations need tools that monitor and assess activities associated with authorized credentials. Some such tools include user activity monitoring (UAM) solutions that record and analyze user interactions with and use of applications, databases, and other information resources. The need for such tools is increasingly recognized, even by data protection authorities.[2]

In this report, we provide practical guidance on how organizations can navigate the legal requirements for deploying global UAM and other monitoring solutions. The compliance requirements across the globe for such activities vary. Some jurisdictions permit organizations to engage in a broad range of monitoring activities, particularly when focused on cyber risk management. Other jurisdictions impose substantial limitations on monitoring.

In Sections I and II, we look at the legal issues associated with monitoring workforce activities. Section II also includes a table that presents the estimated levels of compliance effort ("Basic," "Moderate," or "Significant") required to implement certain monitoring activities in 15 countries. In Section III, we address leading practices that organizations can adopt to support compliant deployments of workforce monitoring tools such as UAM. And in Part IV, we present high-level summaries of the legal frameworks impacting workforce monitoring in each of the 15 countries.

We hope that this white paper is a useful resource for all types of organizations as they work to address the threats facing IT systems and data.

---

[1] The authors are Senior Counsel and Counsel, respectively, at the global law firm of Hogan Lovells. Special thanks are owed to the international team of colleagues who provided us with firsthand insights on the dynamic state of laws in this area, including: Melissa Fai (Australia), Isabel Carvalho (Brazil), Paula Pagani (Brazil), Zeinab Yousif (Canada), Mikko Manner (Finland), Johanna Lilja (Finland), Patrice Navarro (France), Julie Schwartz (France), Christian Tinnefeld (Germany), Massimiliano Masnada (Italy), Elisabetta Nunziante (Italy), Joke Bodewits (Netherlands), Wout Olieslagers (Netherlands), Zechariah Chan (Singapore), Gonzalo Gállego (Spain), Laur Badin (Spain), Victor Mella (Spain), Niklas Sjöblom (Sweden), Sandra Torpheimer (Sweden), Julia Bhend (Switzerland), Susen Aklan (Turkey), Eduardo Ustaran (United Kingdom), and Sabrina Salhi (United Kingdom).

[2] *See*, *e.g.*, Off. Privacy Comm'r Canada, Investigation into Desjardin's Compliance with PIPEDA Following a Breach of Personal Information Between 2017 and 2019 (Dec. 14, 2020) ("An organization [that] handles a large volume of transactions involving sensitive personal information [] must have an active monitoring system."), *available at* https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/.

This information is not intended as legal advice and may not apply to any specific factual or legal circumstances. No attorney-client relationship is formed nor should any such relationship be implied. If you require legal advice, please consult with an attorney licensed to practice in your jurisdiction.

I. Introduction

Cyber incidents pose substantial business and legal risks to all types of organizations. Unauthorized access to or use of information assets could lead to government investigations, regulatory actions, and private litigation, including class actions. The fallout from a cyber incident could tarnish an organization's reputation, diminish customer loyalty, hurt partner relationships, or negatively impact stock price or market value.

And the risk landscape is changing. The COVID-19 pandemic, improved information technologies and infrastructure, and economic factors related to real estate costs and costs of living are driving increased adoption of agile working arrangements. For many organizations, a substantial portion of the workforce now works from remote locations. Some organizations are hiring personnel without ever meeting them in person. This creates challenging cyber risk issues.

When an organization's workforce is remote, you may know that the users on the network are using authorized credentials. But you may not know who is using those credentials or whether they are engaging in authorized behavior.

Threat actors may acquire authorized credentials via phishing attacks or other exploits. Or they may take possession of devices that are logged in. New hires may turn out to be members of recruitment infiltrator cells that seek to become trusted users of the organization's information resources, leveraging the access to engage in unauthorized activity. Or trusted employees may become compromised or tricked into engaging in harmful activities.

An effective cyber risk management program should therefore include the use of capabilities designed to detect, prevent, and investigate such cyber incidents.[3] Those tools may include user activity monitoring (UAM) solutions. UAM involves monitoring and recording user activities, such as interactions with data, applications, and networks. UAM solutions 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

Some UAM solutions rely solely on the collection and processing of metadata, such as recording access to applications, session lengths and times, types of data accessed, the size of uploaded and downloaded files, and the destinations of communications. Metadata can reveal potentially suspicious activity. If a user copies text to a new document, takes a screenshot while accessing an application that processes sensitive information, and soon thereafter accesses a personal cloud account, that may suggest potential unauthorized activity, even if the specific content accessed is not known.

Recognizing that what is normal conduct for one user may reflect anomalous activity for another, some UAM solutions enable organizations to identify when user activities diverge from normal routines on a user-by-user basis. For example, an organization may expect an employee responsible for generating certain weekly reports to access a financial database late on Friday nights. However, if an employee in marketing were to access the database late on a Monday night, that may indicate suspicious activity, which could be flagged by certain UAM solutions.

---

[3] Major industry-level standards and frameworks recognize the need for such monitoring. See, for example, the ISO 27000 family of information security management standards as well as 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/cyberframework.

Regardless of whether UAM solutions process metadata, content, or personal information, they likely implicate laws or regulations governing privacy and data protection, communications secrecy, or employment. These laws and regulations are far from consistent.

Not all UAM solutions rely solely on metadata. Some involve the collection and processing of personal information or the contents of private communications sent or received by employees. And regardless of whether UAM solutions process metadata, content, or personal information, they likely implicate laws or regulations governing privacy and data protection, communications secrecy, or employment. These laws and regulations are far from consistent, as reflected in the table following Section II and the high-level summaries of workforce monitoring legal frameworks in each of 15 countries presented in Section IV.

As discussed further in Section III, though, organizations can take reasonable steps to support the deployment of UAM. For example, in addition to having an overall privacy program, organizations can mitigate privacy risk by deploying UAM solutions that flag suspicious activities without directly identifying users, such as by relying on pseudonymous identifiers.[4] And organizations may be able to configure UAM solutions to only process metadata in some jurisdictions, while enabling the processing of content information in others. Such flexibility may help organizations mitigate the impacts of privacy and data protection, communications secrecy, and employment laws, while continuing to address cyber risk.

II. Legal Considerations for UAM

There are three main areas of law governing the deployment of workforce monitoring tools such as UAM solutions: data privacy and data protection, communications secrecy, and employment. There are substantial differences in these laws across the globe. Some jurisdictions, such as the United States, emphasize the importance of addressing cyber risk and permit organizations to engage in broad monitoring activities so long as the information is processed for cybersecurity purposes. Other jurisdictions, such as Finland, emphasize respect for the privacy interests or labor rights of the workforce, limiting and substantially restricting the scope of monitoring. In this Section, we provide a high-level summary of the legal issues that may affect the deployment of UAM solutions. And we then provide a table summarizing the levels of effort required to engage in certain UAM activities in 15 countries.

Data privacy and data protection laws

UAM solutions often collect personal information (i.e., information relating to an individual who is reasonably identified, directly or indirectly, by the information). For example, UAM data often reflects specific activities undertaken by identified or identifiable individuals in the environment being monitored. The processing of such information is governed by data privacy and data protection laws.

Our review of the 15 jurisdictions addressed in this report reveals an overarching principle for purposes of data privacy and data protection compliance: the deployment of UAM solutions can be evaluated by assessing whether they address cyber risks in a manner that reflects a reasonable balance between the privacy interests of the workforce and the organization's interests in managing cyber risks. The key questions organizations should ask are:

Our review of the 15 jurisdictions addressed in this report reveals an overarching principle for purposes of data privacy and data protection compliance: the deployment of UAM solutions can be evaluated by assessing whether they address cyber risks in a manner that reflects a reasonable balance between the privacy interests of the workforce and the organization's interests in managing cyber risks.

- Is the UAM solution intended to address identified cyber risks?
- Will the UAM solution effectively address the identified risks?
- Are there other solutions that could effectively address the identified risks 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?

A German data protection authority's recent action taken against an employer for deploying video monitoring tools demonstrates how the test of reasonableness may be applied in practice. The

[4] Pseudonymous identifiers are those that cannot be attributed to a specific individual without the use of additional information, particularly in circumstances where the additional information is subject to technical and organizational measures designed to prevent identification of individuals except where reasonably necessary for specified purposes.

employer allegedly deployed video cameras in the workplace for purposes of investigating potential criminal activity and other reasons. Video surveillance may very well be an effective means of addressing the risk of theft. However, the data protection authority claimed that the company should have considered whether less intrusive means (such as random bag checks) would have been effective. And the data protection authority claimed that the retention of recordings for 60 days was significantly longer than necessary. Concluding that the impacts on employees outweighed the benefits to the employer, the data protection authority has fined the employer 10.4 million Euros.[5]

The approach reflected in this enforcement action generally aligns with the 2017 guidance of the EU-wide data privacy regulatory board formerly known as the Article 29 Working Party[6] regarding how to comply with then-current European Union data protection laws in association with workforce monitoring. The European Data Protection Board (EDPB), which is responsible for issuing guidance regarding compliance with the current General Data Protection Regulation (GDPR), has not formally adopted that guidance document, nor has the EDPB published its own guidance regarding workforce monitoring. However, the Article 29 Working Party guidance continues to be a useful resource, as the GDPR built upon prior laws rather than creating an entirely new data protection framework.

The Article 29 Working Party guidance recognized that workforce monitoring solutions can help organizations address cyber risk and discussed how organizations should assess the deployment of workforce monitoring solutions. Of particular interest in connection with the deployment of UAM solutions, the guidance noted that the privacy impact of monitoring can be reduced by measures such as:

- Using automated tools to detect anomalies in workforce use of information resources that are associated with potential, specific threats, and flagging employee activities for review *only* where anomalies are found.
- Providing workforce members with clear information about the types of monitoring that will be conducted and what types of activities may prompt further investigation.
- Recording the minimum amount of information needed to address the identified risks.
- Deploying tools so that they prioritize preventing rather than recording misuse or resources or unauthorized activities (e.g., warning workforce members that they may be about to violate applicable policies rather than recording that workforce members have violated such policies).

It must be emphasized that the test of reasonableness recommended in the guidance and reflected in the German data protection authority's enforcement action is highly fact-specific. Whether a particular measure is reasonable will depend, among other things, on the effectiveness of the measure, the sensitivity of the information collected, the nature and sensitivity 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.

Where UAM solutions involve technologies that support automated decisionmaking or profiling–analyzing or predicting employee activities to assess risk–organizations should take particular care to confirm that such processing complies with legal requirements. Under the GDPR and similar laws, employees have a right to object to decisions made solely on the basis of automated processes that have significant impacts (e.g., affecting employment decisions). If UAM solutions may trigger such impacts (e.g., suspensions or terminations), it will be prudent for organizations to incorporate human decisionmaking into the process.

Additionally, automated decisionmaking processes may leverage machine learning, artificial intelligence, or similar technologies. These technologies may be prone to bias, potentially producing results that have the effect of discriminating on the basis of inherent characteristics such as gender or race.[7] Organizations should seek assurance that UAM solutions are being deployed in such a manner as to avoid having unlawful or unwanted discriminatory impacts.

Communications secrecy laws

UAM solutions may involve monitoring workforce use of electronic communications networks and tools. Many jurisdictions have adopted laws that generally permit organizations to intercept or record

---

[5] Lower Saxony Data Protection Authority, Press Release (Jan. 8, 2021) (in German), https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html.

[6] Article 29 Working Party, Opinion 2/2017 on data processing at work (2017).

[7] Jasmine Henry, *Biased AI Is Another Sign We Need to Solve the Cybersecurity Diversity Problem*, Security Intelligence (Feb. 6, 2020), https://securityintelligence.com/articles/biased-ai-is-another-sign-we-need-to-solve-the-cybersecurity-diversity-problem/.

the contents of communications if at least one party to the communication consents, with some jurisdictions requiring the consent of all parties. Some of those jurisdictions permit organizations to intercept or record the content of communications without consent when such activities are focused appropriately on legal compliance, preventing criminal activities, or addressing information or network security.

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

Employment laws

In some jurisdictions, particularly in the European Union, organizations must consult with or obtain consent from employee representative bodies (e.g., works councils) prior to deploying UAM solutions. Organizations subject to such requirements should budget adequate time for these interactions as they can take weeks or even months to resolve. Some jurisdictions, such as Italy, may require organizations to obtain approvals from or register UAM programs with employment authorities.

Section IV of this White Paper contains high-level summaries of how employment, communications secrecy, and data privacy/data protection laws impact the deployment of UAM solutions in 15 countries. On the next page, we provide a table reflecting the estimated levels of effort required to engage in specified UAM activities in those jurisdictions. And in Section III, we offer some approaches that organizations can adopt to support compliance when deploying UAM solutions.

Table. Legal Compliance Effort to Implement Workforce Monitoring for Cyber Threat 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**	**Brazil**	**Canada**	**Singapore**	**Turkey**	**United States**
Compliance Effort Overall[8]	*Substantial*	*Substantial*	*Substantial*	*Substantial*	*Moderate*	*Substantial*	*Moderate*	*Substantial*	*Moderate*	*Basic*	*Moderate*	*Moderate*	*Basic*	*Moderate*	*Basic*
Monitoring temporal metadata (e.g., logon, logoff, session length)	3	3	4	4	1	3	4	2	1	1	2	1	2	1	1
Monitoring use of privileged access (e.g., administrator accounts)	3	3	3	3	2	3	2	3	2	1	2	2	1	2	1
Monitoring use of applications	5	3	4	4	2	3	4	4	2	1	3	2	1	2	2
Monitoring email communications	5	4	4	4	3	5	4	4	3	2	3	3	2	4	2
Monitoring employer-provided devices	5	4	4	4	3	5	4	4	3	2	3	3	2	3	2
Monitoring Internet browsing	5	4	4	5	4	5	4	4	4	2	2	3	2	4	2
Capturing on screen activities	5	5	5	5	4	5	4	5	3	2	3	4	4	4	2
Keylogging	5	5	5	5	5	5	4	5	5	2	3	4	4	4	2
Monitoring behavior on social media and other channels	5	5	4	4	5	5	4	5	5	4	5	4	2-4	4	3
Monitoring employee-owned devices	5	5	5	5	4	5	5	4	4	4	4	4	4/5	4	3
Total	46	41	42	43	33	44	39	40	32	21	30	30	24-27	32	20

[8] ***Compliance Effort Overall*** is an approximate characterization of the level of compliance resources required to implement the related activity 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 "Substantial." These ratings are provided for illustrative purposes only. For more information consult the detailed descriptions in 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. Approaches to Achieving Compliance

The patchwork of laws affecting the deployment of global cyber defense programs involving UAM can make compliance seem daunting. However, there are steps organizations can take to navigate the challenges. Organizations can benefit from the following:

- *Identifying the threats the organization seeks to address.* In many jurisdictions, the lawfulness of UAM will depend, at least in part, upon whether the deployment is focused on addressing specific, reasonable threats. Documenting in advance of deployment the risks that UAM solutions are intended to address, and the ways in which they will do so, will help support further compliance activities.

- *Identifying relevant jurisdictions involved.* Organizations can better focus the design of cyber risk programs and the selection of UAM solutions by first identifying the relevant jurisdictions. Some solutions, such as keyloggers, may be effective at addressing specific risks. But they may be prohibited or burdensome to deploy in certain jurisdictions.

- *Convening a cross-functional team to oversee the selection, deployment, and operation of cyber defense programs and UAM solutions.* Such a team could be comprised of representatives from across the organization, including Information Security, Information Technology, Legal, Compliance, and Human Resources. And it may be useful to include representatives from key jurisdictions or regions. Such a cross-functional, multi-jurisdictional team can help assess and navigate relevant compliance, operational, and cultural issues.

- *Promulgating policies.* Once organizations have chosen the UAM solutions they wish to use and determined how they want to use them, they should develop, publish, and train employees on the policies that will govern the use of the solutions. Such policies should, among other things, establish roles and responsibilities for managing and operating solutions, limit authorized access to information collected via the solutions, and establish information retention and disposal requirements.

- *Adopting a compliance workplan.* Depending upon the jurisdictions involved, organizations may need to address a range of compliance issue, such as: configuring UAM solutions to capture only metadata or aggregate information; consulting with employee representative bodies; obtaining employee consents; engaging vendors; and addressing international data transfer requirements. Recruiting project management resources to oversee the execution of the workplan may be beneficial.

In addition, organizations should consider the following:

Additional data protection requirements

Those may include:

- Conducting privacy or data protection impact assessments designed to identify and minimize privacy or data protection risks;
- Providing transparent notices about the processing of information;
- Obtaining employee consent;
- Developing records of data collection, storage, use, and sharing;
- Addressing restrictions on transferring personal information to other countries;
- Implementing processes to address employee rights regarding personal information (e.g., rights of deletion and access); and
- Confirming that third parties involved in the deployment or operation of UAM solutions are engaged subject to appropriate agreements addressing data processing obligations.

Socializing the use of UAM solutions with employees

Without context, employees who become aware of the use of UAM solutions may be concerned that their activities and performance are subject to continuous surveillance. This may have a chilling effect on the workforce or otherwise adversely impact morale. To address this risk, organizations may want to socialize the organization's reasons for deploying UAM solutions and the ways in which the solutions will be deployed.

Organizations can help employees understand the specific risks facing their organizations and the ways in which UAM solutions can address those risks. When appropriate, organizations can describe how UAM solutions help employees avoid missteps, such as by prompting employees to confirm whether they wish to send an attachment to an external email account or by blocking interactions to potentially malicious.

Organizations that deploy and explain their cyber risk programs in terms of protecting the organization and its workforce (rather than focusing on catching wrongdoers) can bolster trust and support for the deployment of UAM solutions.

Organizations that deploy and explain their cyber risk programs in terms of protecting the organization and its workforce (rather than focusing on catching wrongdoers) can bolster trust and support for the deployment of UAM solutions.

Consider pseudonymization

Pseudonymization involves processing personal information in a way such that the individuals to whom the personal information relates cannot reasonably be identified without the use of additional information. For example, the direct identifier JaneDSmith could be replaced with the pseudonymous identifier X3452AFO. When the lookup table or additional information used to associate the pseudonymous identifier with identifiable data is maintained separately from the new identifier, pseudonymization can be an effective means of mitigating data privacy or data protection risk.[9]

Deploying UAM solutions in a pseudonymous manner may help organizations address compliance obligations and workforce concerns. For example, organizations may be able to configure UAM solutions so that they flag suspicious activity associated with a user identified only by pseudonymous information. With the right controls in place, security teams monitoring UAM signals may not be able to identify specific employees associated with suspicious activities. If security teams identify signals that appear to be valid and of concern, they can pass the information along to legal, compliance, human resources, or other teams that will determine whether further action is needed and whether individual users should be identified.

Pseudonymization can therefore help organizations deploy UAM solutions in ways that satisfy the test of reasonableness. The potential privacy impacts of UAM are reduced when the information does not readily identify employees and when the identities of employees are revealed only when there is evidence of misconduct or other activities that warrant further action.

[9] *See* Art. 25, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), OJ 2016 L 119/1.

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 a specific organization is 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
- Brazil
- Canada
- Singapore
- Turkey
- United States

FINLAND

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

In Finland, the privacy of communications is a fundamental right. Under Finnish law, the general rule is that employers may process electronic communications and traffic data (i.e., metadata) only with the consent of all parties to the communications unless specifically permitted by law. Employers are not considered parties to communications, even if communications are sent to or from applications or tools provided by employers solely for business purposes.

Exemptions to the confidentiality of communication are interpreted narrowly. Employers generally may not monitor the *contents* of employees' electronic communications. Finnish law allows employers to process traffic data related to employees' electronic communications for the purposes of: detecting, preventing and investigating cases of misuse of the communications service or network or the disclosure of business secrets (subject to specific limitations); ensuring information security (subject to specific limitations); and detecting technical faults or errors (subject to specific limitations).

Employers may use automated tools to monitor traffic data for purposes of preventing or investigating the installation of unauthorized devices, services, or software on employer networks; unauthorized access to employer networks; or similar misuse of employer resources as defined in acceptable use policies presented to employees if such acts or events likely would cause substantial adverse impacts.

Employers may use automated tools to monitor traffic data for purposes of preventing or investigating the installation of unauthorized devices, services, or software on employer networks; unauthorized access to employer networks; or similar misuse of employer resources as defined in acceptable use policies presented to employees if such acts or events likely would cause substantial adverse impacts.

Employers may manually process traffic data if there are reasonable grounds to suspect that a communications network or service is subject to misuse that likely would cause substantial adverse impacts. Employers may process only such data as is necessary for investigating the unauthorized use and the parties responsible for it and for ending the unauthorized use.

Employers technically are permitted to use automated tools to monitor traffic data in a manner that does not readily facilitate the identification of individuals for the purposes of preventing or investigating the disclosure of substantial business secrets. If there are reasonable grounds to suspect that such a business secret has been disclosed to a third party without permission via a communications network or communications service, manual review of traffic data that identifies individuals may be permitted in certain limited circumstances. 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 for these purposes and must provide annual reports to these entities. As a result of these requirements, few companies have implemented such monitoring.

Employers may however 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) the 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).

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; 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: *Strict limits on processing communications data.*
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.*

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.

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.

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 notify employees about: (1) the types of personal data that will be collected; (2) the purposes of collection; (3) the legal basis of the processing; (4) the retention of personal data; (5) the recipients, if any, of the personal data; (6) the possible transfer of personal data outside the EU; (7) their rights regarding personal data; and (9) the contact information for entities controlling the processing of the data. If employers adopt acceptable use policies that include potential sanctions for violations, the policies must be distributed to employees after consulting with staff representatives, if any, filed with the Labour Court, and submitted to the Labour Inspector for review.	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.

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, a Data Protection Impact Assessment (DPIA) likely will be required, particularly for systematic monitoring programs (e.g. Data Loss Prevention). 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, data transfer restrictions and security measures. Employers should retain personal data captured via monitoring for no more than six months. Employers must consult with staff representatives (*Comité Social et Economique*) that may be established in the work place; and inform employees before introducing monitoring technologies.

Employers must 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 French Labor Code, French Data Protection Authority (CNIL)'s guidelines.

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; carry out a DPIA; notify employees; and submit acceptable use policies that include sanction provisions 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; carry out a DPIA; notify employees; and submit acceptable use policies with sanction provisions to the Labor Inspector.*
Monitoring use of applications	*3: Metadata only. Prior consultation with all competent staff representatives; carry out a DPIA; notify employees; and submit acceptable use policies with sanction provisions to the Labor Inspector.*
Monitoring email communications	4: *Avoid processing personal communications. Prior consultation with all competent staff representatives; carry out a DPIA; notify employees; and submit acceptable use policies with sanction provisions to the Labor Inspector.*
Monitoring employer-provided devices	4: *Avoid processing personal communications. Prior consultation with all competent staff representatives; carry out a DPIA; notify employees; and submit documents to the Labor Inspector.*
Monitoring Internet browsing	4: *Prior consultation with all competent staff representatives; carry out a DPIA; notify employees; 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. Prior consultation with all competent staff representatives; carry out a DPIA; notify employees; and submit acceptable use policies with sanction provisions 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. Prior consultation with all competent staff representatives; carry out a DPIA; notify employees; and submit acceptable use policies with sanction provisions 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.

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 (but employers may need to consult with the works council).

Notification Considerations	Consent Considerations
Employers must notify employees about: (1) the types of personal data that may be collected and further processed; (2) the purposes of collection and processing; (3) how the data will be used; (4) the retention of personal data; (5) the recipients, if any, of personal data; (6) the employee's rights as a data subject; (7) the legal basis of processing; and (8) the name and contact details of the controller (i.e., the employer) and the data protection officer (DPO). If employers obtain consent to monitoring, such notice must be included in a consent declaration form. A separate notice is not required in these circumstances. The consent form must inform employees that they can revoke their consent at any time, noting the consequences for doing so, which may include revocation of the right to use certain applications or tools.	Consent can serve as the basis for reasonable monitoring activities that involve the processing 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. 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.

German data protection authorities (DPA) have a strict view on the lawfulness of employee data processing, and there is a tendency of (former) employees and works councils to lodge complaints at the DPAs or use data privacy concerns as a legal argument in legal disputes and labor court proceedings.

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.

German data protection authorities (DPA) have a strict view on the lawfulness of employee data processing, and there is a tendency of (former) employees and works councils to lodge complaints at the DPAs or use data privacy concerns as a legal argument in legal disputes and labor court proceedings.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work; Baden-Wuerttemberg DPA guidance (in German).

Notable Laws or Regulations. Federal Data Protection Act; General Data Protection Regulation; 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 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 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.

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 certain circumstances where employers have legitimate suspicions of illicit activities and monitoring is conducted to identify misconduct and protect company assets. The requirement to obtain agreement with trade union representatives or authorization from local employment office does not apply to the deployment of technologies that employees must use to perform work activities or to technologies that register attendance. However, if such technologies collect more information than necessary to support those purposes, labor union or employment office agreements may be required.

Monitoring technologies and programs that process of personal data must collect, retain, and use personal data only as necessary to accomplish legitimate interests that are not outweighed by the adverse impact on employee privacy interests. Prior to deployment, employers should assess the processing activities related to monitoring to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impacts on employees.

According to the Italian Data Protection Authority, employers should conduct data protection impact assessments for monitoring activities, particularly those that involve systematic monitoring of publicly accessible areas or innovative technological or organizational solutions.

Employers should retain personal data collected for monitoring purposes only as strictly necessary to achieve specified purposes. Employers may not record employees' attempts to access inappropriate web sites. Employers may retain communications metadata 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, in compliance with the general principles of necessity and proportionality especially with regard to possible private communications or documents of the employees.

Notification Considerations	Consent Considerations
Employers must provide employees with clear notice compliant with all requirements of art. 13 of the GDPR, particularly including: (1) the types of personal data that may be collected; (2) the purposes and legal basis of collection and processing of data; (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, with specific regard to the extent resources can or cannot be used for private purposes.	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. Employers that implement monitoring tools in line with the restrictions noted above may engage in monitoring without obtaining consent.

Additional Considerations.

Employers must address other relevant data protection obligations, including complying with appropriate employee requests to exercise their rights, data transfer restrictions, privacy by default measures, and contractual arrangements and specific instructions to suppliers acting as data processors.

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; 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 in limited circumstances.*
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.*

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 and continuously monitoring employees 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 access to monitoring data is limited and that monitoring data is retained no longer than necessary. Six months is generally regarded as an acceptable maximum retention period for this purpose.

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 and continuously monitoring employees may be considered disproportionate.

Covertly monitoring employees (without notifying them in advance) could only be deployed when there is a legitimate suspicion of unlawful conduct and there are no other reasonable means to investigate and address the suspicions. Employers should notify employees after completing covert monitoring activities.

Recent guidance and enforcement actions of the Dutch Data Protection Authority (Dutch DPA) show that employers should be cautious when deploying access control measures that make use of biometric data, such as fingerprints or iris scans. This is generally only allowed in situations where (i) employees can freely give explicit consent without any fear of negative consequences or (ii) this is necessary for authentication or security purposes. Both situations should be interpreted strictly.

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 notify employees in advance regarding monitoring that involves the processing of personal data unless there are legitimate suspicions of criminal misconduct or substantial malfeasance (see above). 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) the legal basis of the processing; (5) the retention of personal data; (6) the recipients, if any, of personal data; (7) the possible transfer of personal data outside the EU; (8) their rights regarding personal data; and (9) the contact information for entities controlling the processing of the data.	Employee consent is generally not considered a valid legal basis for monitoring as the employment relationship is deemed to preclude employees from providing freely given consent.

Additional Considerations. Prior to deployment, employers should, amongst others, assess their insider threat programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Furthermore, conducting a Data Protection Impact Assessment (DPIA) is required prior to monitoring employees on a *large scale*. Conducting a DPIA is always required (also when the large scale threshold is not met) in case of covertly monitoring employees. If the DPIA indicates that the monitoring would result in a high risk in absence of measures to mitigate the risk, the competent DPA should be consulted. 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. Dutch DPA, Online Guidance on Monitoring Employees (available in Dutch only).

Notable Laws or Regulations. General Data Protection Regulation; Dutch Implementation Act to the GDPR; Dutch Telecommunications Act; Universal Service and End User Interests Decree; Works Councils Act.

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, unless and to the extent that the monitoring is necessary for protecting the integrity and security of the network or service.*
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 business applications.*
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., with 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., with 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, among other obligations, the test of reasonableness. This test involves determining whether monitoring effectively achieves a legitimate 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.

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

Additionally, employers should provide employees with clear notices that limit or even eliminate any expectations of confidentiality or privacy that employees may have regarding their use of communications resources.

Employers may access information regarding employee use of company-provided devices solely for purposes of confirming that employees are fulfilling their employment obligations or safeguarding devices and the information stored on or accessed via the devices. Employers must coordinate with employee representatives to establish policies regarding such access to protect employees' privacy interests. If employers permit employees to use company-provided devices for personal use, employers must: (i) provide acceptable use policies to employees before engaging in monitoring; and (ii) establish policies designed to protect employee privacy interests, such as by clarifying when employees may use devices for personal purposes.

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 notify employees about: (1) the types of personal data that will be collected; (2) the purposes of collection; (3) the legal basis of the processing; (4) the retention of personal data; (5) the recipients, if any, of the personal data; (6) the possible transfer of personal data outside the EU; (7) their rights regarding personal data; and (9) the contact information for entities controlling the processing of the data.	Except in 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 monitoring programs to confirm that the legitimate purposes for the programs are not outweighed by the potential adverse impact on employees. Employers should confirm that they address other relevant data protection obligations, including complying with appropriate employee requests to access, rectification, erasure, limitation of processing, portability of data and objection.

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 (a scenario that rarely occurs in the context of an employee-employer relationship).

Employers likely will have to carry out a data protection impact assessment prior to the implementation of any monitoring tools. The Spanish Data Protection Authority has published a Black List of activities that would require such an assessment.

Official Guidance. Article 29 Working Party, Opinion 2/2017 on data processing at work; DPIA Black List issued by the Spanish Data Protection Authority (in Spanish only).

Notable Laws or Regulations. Spanish Data Protection Act 3/2018 of 5 December on the protection of personal data and guaranteeing digital rights; General Data Protection Regulation; 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)	3: *Metadata only. So, impact is reduced.*
Monitoring use of privileged access (e.g., administrator accounts)	3: *Estimate based on likelihood that little personal data will be involved and increased justification for monitoring administrative access.*
Monitoring use of applications	3*: Metadata only. So, impact is reduced.*
Monitoring email communications	5*: Conduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority) and provide clear notice as detailed above.*
Monitoring employer-provided devices	5: *Conduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority) and provide clear notice as detailed above.*
Monitoring Internet browsing	5: *Conduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority) and provide clear as detailed above notice. Presumption of higher expectation of privacy.*
Capturing on-screen activities	5: C*onduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority)and provide clear notice as detailed above. Presumption of higher expectation of privacy.*
Keylogging	5: *Conduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority)and provide clear notice as detailed above. Presumption of higher expectation of privacy.*
Monitoring behavior on social media and other channels	5: *Conduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority)and provide clear notice as detailed above. Presumption of higher expectation of privacy.*
Monitoring employee-owned devices	5: *Conduct data protection impact assessment (in accordance with the DPIA Black List issued by the Spanish Data Protection Authority) and provide clear notice (in particular, a specific "Bring Your Own Device" policy). 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. Furthermore, it is generally not permitted to use an IT system to regularly monitor employee performance.

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 notify 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) the purposes of collection; (3) the legal basis or processing; (4) the retention of personal data; (5) the recipients, if any, of the personal data; (6) the possible transfer of personal data outside the EU; (7) their rights regarding personal data; and (8) the contact information for entities controlling the processing of the data.	According to the Swedish Data Protection Authority, consent is not a lawful basis for the processing of personal data for purposes of employee monitoring.

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 should 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 revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) unless there is a legal obligation to process the information or if it is necessary to protect certain vital interests. Employers may generally not process personal data relating to criminal convictions and offences unless the processing is necessary for legal claims to be established, asserted or defended, the processing is necessary in order for a legal obligation under law or regulation to be fulfilled, or if the personal data refers to persons in key positions within the own company or company group and it is the data refer to persons in key positions or leading position within the own company or group and it is objectively justified to process the data in specially set up reporting channels to investigate the person in question has been involved in serious irregularities relating to accounting, auditing, bribery, banking and finance related crime, or other serious irregularities relating to the vital interests of the organization or the lives of individuals and health.

Personal data may not be stored longer than is necessary to fulfill the legitimate purposes of the processing. 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. The Swedish Data Protection Authority, DIFS 2018:2 Regulation on the processing of personal data concerning criminal offences (only in Swedish); The Swedish Data Protection Authority, List regarding Data Protection Impact Assessments according to article 35.4 of the General Data Protection Regulation; Article 29 Working Party, Opinion 2/2017 on data processing at work.

Notable Laws or Regulations. Act containing supplementary provisions to the EU General Data Protection Regulation (SFS 2018:218); Ordinance containing supplementary provisions to the EU General Data Protection Regulation (SFS 2018:219) (only in Swedish); The Criminal Data Act (SFS 2018:1177) (only in Swedish); General Data Protection Regulation; Co-Determination in the Workplace Act (non-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)	4: *Data protection impact assessment due to potential impact on employees*.
Monitoring use of privileged access (e.g., administrator accounts)	2: *Data protection impact assessment required. Estimate based on likelihood that little personal data will be involved and heightened risks associated with administrative access.*
Monitoring use of applications	4*: Data protection impact assessment due to potential impact on employees*.
Monitoring email communications	4: *Data protection impact assessment due to potential impact on employees*.
Monitoring employer-provided devices	4: *Data protection impact assessment due to potential impact on employees*.
Monitoring Internet browsing	4: *Data protection impact assessment due to potential impact on employees*.
Capturing on-screen activities	4: *Data protection impact assessment due to potential impact on employees*.
Keylogging	4: *Data protection impact assessment due to potential impact on employees*.
Monitoring behavior on social media and other channels	4: *Data protection impact assessment due to potential 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).

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).

Additional Considerations. Employers should 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.

Pursuant to the revised Federal Data Protection Act, that will likely come into force in 2022, 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: Guide to Internet and Email Monitoring in the Workplace (German); Guide to Processing Personal Data at Work (German).

Notable Laws or Regulations. Federal Data Protection Act (which will be modified in light of the General Data Protection Regulation); Ordinance to the Federal Data Protection Act; Swiss Criminal Code; Telecommunications Act; Ordinance on Telecommunication Services; 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 employees' activities.*
Monitoring behavior on social media and other channels	5: *Likely prohibited except in 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 tools that do not capture personal data are not subject to the restrictions of data protection law.

Monitoring that involves the interception of communications during transmission, is governed by the 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 notify 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) the legal basis of the processing; (5) the retention of personal data; (5) the recipients, if any, of the data; (6) the possible transfer of personal data outside the UK; (7) their rights regarding personal data; and (8) the contact information for entities controlling the processing 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. 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.

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.

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. UK General Data Protection Regulation (as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 and its successor laws); General Data Protection Regulation (EU) 2016/679; Data Protection Act 2018; Investigatory Powers Act 2016; Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (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.

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.

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 notify employees regarding 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. 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 continuous or intermittent; and (5) whether surveillance will continue for an extended or limited period. In New South Wales and the Australian Capital Territory, the monitoring must be conducted in accordance with a policy for such monitoring, which must also be notified to the employee in such a way that it is reasonable to assume that the employee is aware of and understands the policy.	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 reflects assumption that monitoring will focus on types of applications used rather than on 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 required due to monitoring out of work activities.*
Monitoring employee-owned devices	4: *Need express consent in certain jurisdictions.*

BRAZIL

General considerations. Monitoring that involves the processing of personal data must satisfy the test of reasonableness and the principles of intimacy, privacy, dignity and non-discrimination. 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.

Legitimate interests for monitoring include detecting or preventing violations of law, regulations, or important internal policies.

Assessing the reasonableness of monitoring is a highly fact-dependent exercise. Legitimate interests 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 illegal.

With regards to corporate emails, Brazilian Labor Courts provide that employers may monitor employee's corporate email accounts. However, monitoring private communications exchanged by other means (e.g., private e-mail accounts and social media websites) is deemed a violation of employee privacy, even when undertaken via corporate devices. Therefore, employees must be clearly informed that corporate devices and email accounts are for business purposes only, and the use of them is subject to monitoring.

Notification Considerations	Consent Considerations
Employers must notify employees in Portuguese regarding monitoring that involves the processing of personal data. 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 period of personal data; and (5) the recipients of personal data, if any.	Consent is not required if monitoring is conducted on the basis of employers' legitimate interests described above. Employees must be provided with clear notice. Consent might justify monitoring that goes beyond what is reasonably necessary to accomplish legitimate business purposes. Consent must be freely given, which may be difficult to establish in the employment context. Employees would have the right to withdraw consent, thereby interfering with 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. Monitoring that involves the processing of sensitive information (i.e., information relating to race, ethnic origin, political opinions, religious beliefs, trade union membership or sexual orientation) likely will be lawful only if it is necessary to comply with a legal obligation.

Notable Laws and Regulations. Brazilian Data Protection Law (Law No. 13,709) and Brazilian Labor Code (Decree-Law No. 5,452).

Brazil: 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: *Notify employees.*
Monitoring use of privileged access (e.g., administrator accounts)	2: *Notify employees.*
Monitoring use of applications	3: *Notify employees. Employers cannot monitor private communications due to article 5, X of the Brazilian Federal Constitution that protects the right of intimacy and private life.*
Monitoring email communications	3: *Notify employees. Employers cannot monitor private communications due to article 5, X of the Brazilian Federal Constitution that protects the right of intimacy and private life.*
Monitoring employer-provided devices	3: *Notify employees. Employers cannot monitor private communications due to article 5, X of the Brazilian Federal Constitution that protects the right of intimacy and private life.*
Monitoring Internet browsing	2: *Notify employees.*
Capturing on-screen activities	3: *Notify employees. Employers cannot monitor private communications due to article 5, X of the Brazilian Federal Constitution that protects the right of intimacy and private life.*
Keylogging	3: *Notify employees. Employers cannot monitor private communications due to article 5, X of the Brazilian Federal Constitution that protects the right of intimacy and private life.*
Monitoring behavior on social media and other channels	5: *Employers generally cannot monitor private conduct. However, employers may be permitted to monitor publicly-available information to alert employers to activities or behaviors that may cause serious harm to the company.*
Monitoring employee-owned devices	4: *Request employee's consent. Employers cannot monitor private communications due to article 5, X of the Brazilian Federal Constitution that protects the right of intimacy and private life.*

CANADA

General Considerations. Employee monitoring is governed by federal and provincial privacy laws, which focus on the reasonableness of monitoring. Privacy laws may vary depending on the specific jurisdictions implicated.

Generally, employers may engage in monitoring if the monitoring is reasonable, taking into consideration the employer's purpose and the manner in which it is carried out. Specifically, the employer should ascertain whether the monitoring is necessary to satisfy an objective of the employer (e.g. to protect assets or enhance safety), whether it is likely to accomplish the objective, whether the impact on employee privacy is proportional to the benefits gained by the employer, and whether there is no less intrusive means of accomplishing the objective. Less invasive forms of monitoring are more likely to be found reasonable. Employers should generally advise employees of the existence of the monitoring and all the potential uses for the personal information collected. This can be done through a policy. Some jurisdictions will also require employers to identify the purpose of the monitoring, and other information, such as a process by which individuals can request access to their personal information held by the employer. In some circumstances, employers may also be required to obtain advance consent to any monitoring.

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 should 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.

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.

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.

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 is (a) reasonable for the management or termination of employment relationships; or (b) necessary for evaluative purposes (including to evaluate the suitability, eligibility, or qualifications of an employee for promotion or continued employment). In addition, monitoring may take place if the collection of information is necessary for any investigation or proceeding, where seeking the consent of the individual would compromise the availability or the accuracy of the personal data (for example, if an employee is suspected of misconduct and may seek to delete emails or documents).

Using automated tools to flag activities for review only when there are signs of misconduct will likely be considered more reasonable than sampling employee activities for manual review on a general basis.

To assess the reasonableness of monitoring, employers must consider whether a reasonable person would consider the monitoring appropriate in the circumstances. It generally is considered reasonable to monitor an employee's emails on a work email server. And the privacy regulator in Singapore (the PDPC) has confirmed that reasonable purposes falling within (a) above include monitoring employees' use of computer network resources. Using automated tools to flag activities for review only when there are signs of misconduct will likely be considered more reasonable than sampling employee activities for manual review on a general basis.

However, if monitoring captures more information than is necessary to manage or terminate employment relationships, consent likely is required. As such, it is prudent to obtain employee consent to monitor work emails, as such emails will invariably involve the collection of personal data. Employers generally obtain consent through clauses in the employment agreement or the employee handbook, though the former is recommended.

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. Similarly, if monitoring tools are not used to capture personal data (e.g. in certain types of system logging, such as monitoring an employee's access to and use of databases, documents and applications in order to safeguard intellectual property or trade secrets), such tools will not be subject to restriction under Singapore data protection law.

Notification Considerations	Consent Considerations
Employers generally must notify employees about: (1) the types of personal data that may be collected and (2) the purposes for which it will be used (even where no consent is required). Employers should inform employees that company resources 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. 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 generally obtain consent through terms in the employment agreement. However, 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.

Additional Considerations. Employers will want to ensure 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.

Under the Computer Misuse Act (Cap. 50A), which criminalizes certain cyber activities, it would be prohibited for an employer to use an employee's password to access a personal email account without a lawful authorization.

Official Guidance. Personal Data Protection Commission, Advisory guidelines on the PDPA for selected topics (Chapter 5, Employment)

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 and 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.*

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 General Data Protection Regulation; rulings of Turkish Constitutional Court and Court of Appeal precedents; and Labor Code No. 4847.

Employers may engage in monitoring activities that involve the processing of personal data if the activities support employers' legitimate interests that are not outweighed by employee privacy interests.

According to the Turkish Constitutional Court, to establish that monitoring is supported by legitimate interests, employers must;

- Conduct a balancing test to ensure that employers' legitimate interests are not outweighed by the fundamental rights of the employees, particularly with regard to the potential processing of personal activities, such as via Internet monitoring and keylogging;
- Provide employees with notice of the monitoring; and
- Conduct monitoring so that the personal data processed is limited to that needed to achieve the specified purposes.

The balancing test Using automated tools to monitor employee activities for specified purposes and monitoring metadata, rather than contents of communications are examples of practices that may satisfy the balancing test.

Employers must obtain explicit consent if monitoring will 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 notify employees about: (1) the types of personal data that will be collected; (2) how personal data will be collected; (3) the purposes of collection; (4) the legal grounds for processing personal data; (5) the identity of the data controller; (6) to whom and for which purposes personal data may be transferred; and (7) employees' rights regarding their personal data.	Explicit 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. If 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 correct, or delete data, cross-border data transfer restrictions, data security obligations, and registration requirements (if any).

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	4: *May be considered to have a substantial impact on employees.*
Monitoring employer-provided devices	3: *Confirm proportionality.*
Monitoring Internet browsing	4: *May be considered to have a substantial impact on employees.*
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 notify employees in writing of monitoring activities or the collection of personal information. 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 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 the CISA's definitions and protection 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.

Given the breadth of the CISA's definitions and protection 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 morale 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 (such as the California Consumer Privacy Act) 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 clear information about the types of information the employer collects, the purposes for doing so, and the circumstances in which information is collected.	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 implicit 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 email communications	1: *Confirm that monitoring is for a cybersecurity purpose. Metadata is less sensitive than other information.*
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 is for a cybersecurity purpose.*

About the Authors

Harriet Pearson

Senior Counsel, 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

Counsel, 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.

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 world as reflected by our ranking as the only firm to be named Band 1 in *Chambers Global Guide: Data Protection*, 2021. 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 the global cybersecurity leader for user and data protection. Forcepoint's behavior-based solutions adapt to risk in real-time and are delivered through a converged security platform that protects network users and cloud access, prevents confidential data from leaving the corporate network, and eliminates breaches caused by insiders. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of enterprise and government customers and their employees in more than 150 countries. www.forcepoint.com