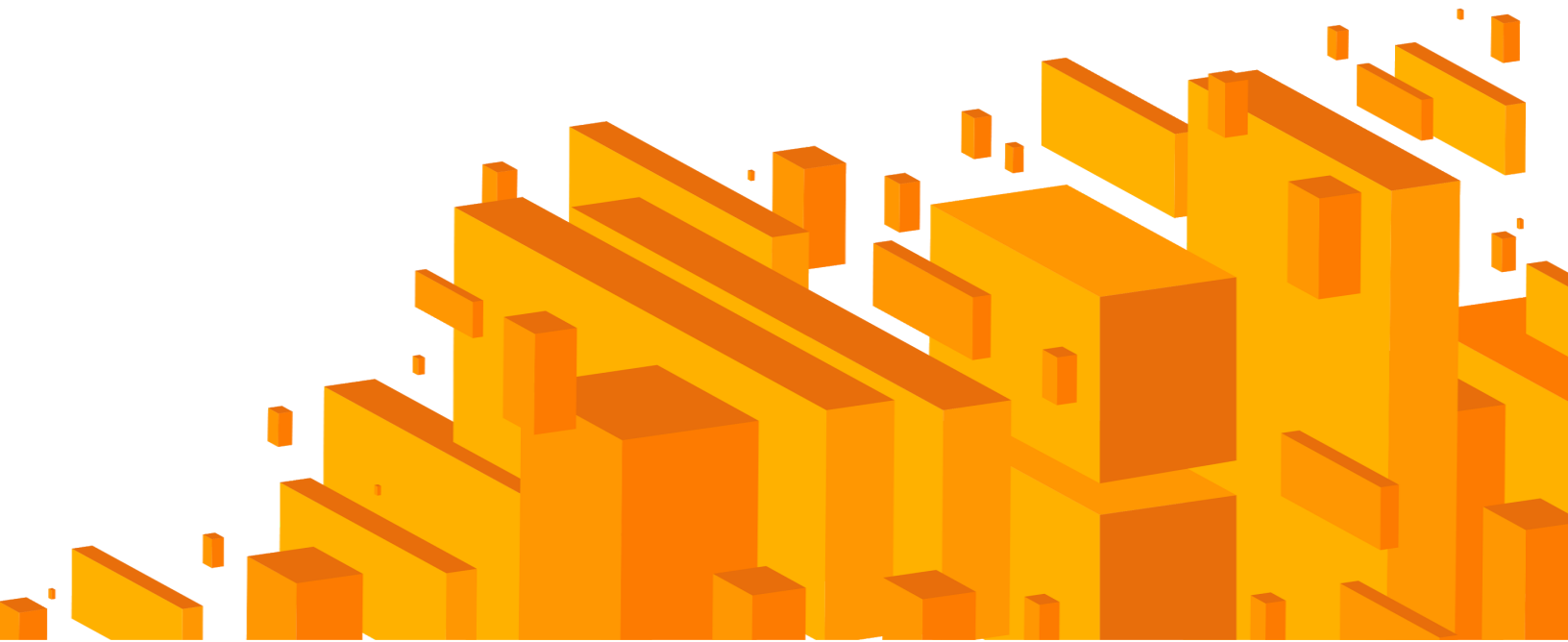
TERAMIND

A Teramind White Paper

Data Privacy in 2020: Identifying, Managing and Preventing Insider Threats in a Privacy-first World

July 2019

The contents of this whitepaper are intended to convey general information only and not to provide legal advice or opinions. The contents of this paper should not be construed as, and should not be relied upon for, legal advice in any particular circumstance or situation. The information presented in this paper may not reflect the most current legal developments. No action should be taken in reliance on the information contained in this article and Teramind disclaims all liability in respect to actions taken or not taken based on any or all of the contents of this paper to the fullest extent permitted by law. Teramind would advise consultation with legal counsel and/or an attorney for advice and legal opinion on specific legal issues.



Introduction 3
Workplace Monitoring 5

Best Practice #1: Understand general principles for monitoring 7

Best Practice #2: Identify the purposes for monitoring 10

Best Practice #3: Monitoring must be proportionate 12

Best Practice #4: Consultation 13

Best Practice #5: Implement technology that fosters compliance 14

Best Practice #6: Understand the monitoring laws of each country 17

Data Protection Laws 18

Oceania 19
Australia 19

Europe 22
Belgium 22
France 28
Germany 31
Italy 34
Spain 38
United Kingdom 41

North America 44
Canada 44
Mexico 47
United States 50

South America 54
Argentina 54
Brazil 58
Chile 64

About Teramind 68

Introduction

Insider initiated data breaches are at an all-time high, with all evidence pointing to increased data exposure for the foreseeable future.[1] Organizations around the world continue to turn to technology-based solutions to identify, document and stop data exfiltration attempts and data breaches. There is, however, some concern that these solutions may create a potential conflict with employee and consumer privacy rights.

The General Data Protection Regulation 679/2016 ("GDPR")[2] was implemented in May 2018, with the goal to ensure data privacy rights of European nationals against all entities collecting and leveraging personal data, with severe financial penalties in the event of non-conformance. GDPR caused a ripple effect around the world, with Brazil taking a lead in South America to pass a data privacy bill, California taking the lead in the US to pass the California Consumer Privacy Act (CCPA),[3] and at the time this whitepaper is published, some 10 or more states in the United States, are in the process of proposing data privacy legislation.[4] To ensure conformance with these strict data privacy regulations, organizations turn to technology solutions to implement oversight and to ensure appropriate audit and forensics tools are in place in the event of a breach or violation, with the ultimate goal to protect their customers' and employees' data.

How should executives and law enforcement officials effectively weigh the demands to control and protect their businesses while protecting legitimate privacy rights of employees and others whose personal data is being threatened?

[1]See, The American Management and The Electronic Monitoring & Surveillance Survey http://www.amanet.org/training/articles/The_Latest- on-Workplace-Monitoring_and_Surveillance.aspx (2019).

[2]General Data Protection Regulation, https://gdpr-info.eu/ (2019).

[3]See, California Consumer Privacy Act, https://www.org.ca.gov/privacy/ccoa (2018).

[4]See, https://www.govtech.com/policy/10-States-Take-Internet-Privacy-Matters-Into-Their-Own-Hands.html (2019).

Insider threat and data loss prevention are complex problems and there is no one simple solution that works best in all situations. Clearly, however, employers are turning to data loss prevention and workplace monitoring to address these concerns. [5]

A recent national survey shows that a majority of employers monitor their employees' workplace activities.[6] The surveys by the American Management Association[7] and the ePolicy Institute[8] show the pervasiveness of employee monitoring with more than half (55%) of the employers engaged in monitoring.[9] Employers are motivated by a number of concerns including the risk of data loss, concerns over lawsuits and the increasing role of electronic evidence in government and regulatory agencies' investigations. This whitepaper outlines best practices that should be adopted as part of a comprehensive insider threat detection and data loss prevention program to proactively address data loss while minimizing privacy risks involved in employee monitoring. In addition, it provides insight to the current legal landscape around the world with respect to employee privacy rights.

[5]In this paper, the term *"monitoring"* is used broadly to refer to any reading collection or storage of electronic communications. Monitoring is, therefore, more than the interception of communications in transit. Copying of employee emails for backup or scanning messages to detect viruses are both considered to be monitoring.

[6]See, Privacy Rights Clearinghouse, https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring (2019).

[7]The American Management Association. See www.amanet.org/hma.

[8]The www.epolicyinstitute.com.

[9]See American Management Association.

Workplace Monitoring

Before discussing best practices, however, it is important to understand how the Key Countries examined in this paper govern workplace monitoring. Workplace monitoring in the Key Countries is governed by a variety of privacy laws, rules and regulations. In some Key Countries, such as Germany, the laws on telecommunications regulate the monitoring of email and other electronic communications. In other countries, such as Belgium, an employer's right to monitor employee communications may be governed by collective bargaining agreements, employment contracts or general privacy and data protection legislation.

> "[A]n an individual's browsing history alone is capable of exposing his or her most intimates, like, activities and thoughts ..."
>
> [Employees] may therefore reasonably expect privacy on the information, at least where personal use is permitted or reasonably expected."
>
> **Hon. Justice Morris**
> The Globe and Mail (October 2,2012)

Throughout Europe, however, and some of the other Key Countries, it is important to understand that privacy is treated as a fundamental human right. What does that mean? It means that these fundamental rights cannot be bargained away.

This view of privacy is supported throughout EU:

- Article 8 of the European Convention for the Protection of Human Rights[10] states: "Everyone has the right to respect for his private and family life, his home and his correspondence."

- The Treaty Establishing the European Community[11] requires Member States to respect the fundamental rights guaranteed by the European Convention.

[10]See https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[11]Treaty Establishing the European Community, Feb.7, 1992, O.J. (C 224)1 (1992). (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12002E/TXT.)

- The Europe Union's Charter of Fundamental Rights[12] affirms, [e]veryone has the right to respect for his privacy and her private and family life, home and communications.

Perhaps Commissioner Vera Jourovova said it best when speaking at the Amsterdam Privacy Conference in 2015 where she said that privacy is "more than a 'European' fundamental right, it is a right for 'everyone.'"[13]

Despite the support that privacy receives as a "fundamental right," privacy is not an absolute right. Privacy Rights must be weighed against other competing interests. This was made clear in Copeland v. United Kingdom[14] where the European Court of Human Rights specifically recognized the rights of an employer to control his business and protect his legitimate interests against the employee's privacy rights.

[12]Convention on the Protection of Human Rights and Fundamental Freedoms. Nov. 4, 1950, art. 8, para. 1, 213 U.N.T.S. 221. https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en.

[13]Speech of Commissioner Jourová at the Amsterdam Privacy Conference. The protection of personal data: More than a "European" fundamental right, it is a right for "everyone". (Brussels, 29 October 2015).

[14]45 Eur. Ct, H.R. 235 (2007).

Best Practice #1: Understand general principles for monitoring

On 8 June 2017, the Article 29 Working Party issued an opinion on employee monitoring Opinion 2/2017.[15] The opinion complemented an earlier opinion, Opinion 08/2001 on the processing of personal data in the employment context.[16]

> "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace they do have legitimate expectation of a certain degree of privacy in the workplace."
>
> **Article 29 Working Party**
> Opinion approved on 13 September 2001

The Article WP 29 was a group of representative data protection authorities from across Europe. The Article 29 Working Party has been re-named the European Data Protection Board.[17] The European Data Protection Board ("EDPB") is an EU body in charge of the application of the General Data Protection Regulation (GDPR) as of 25 May 2018. It's made up of the head of each DPA and of the European Data Protection Supervisor ("EDPS") or their representatives. The European Commission takes part in the meetings of the EDPB without voting rights. The secretariat of the EDPB is provided by the EDPS.

The Article WP29 and the EDPS have commented on the imbalance of power between employers and employees. Given the imbalance between the power of employers when compared with the power of employees, employees can only give free consent in

[15]WP29, Opinion 08/2001 on the processing of personal data in the employment context, WP 48, 13 September 2001, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2001/wp48_en.pdf .

[16]WP29, Working document on the surveillance of electronic communications in the workplace, WP 55, 29 May 2002, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2002/wp55_en.pdf.

[17]See, E.U. Commission, "What is the European Data Protection Board?" https://edpb.europa.eu/edpb_en (2018).

exceptional circumstances stances, and so, their consent should not be the sole legal basis for employee authorization.

The Article 29 Working Party's guiding principles for workplace monitoring can be summarized as follows:

- Employees do not lose their privacy and data protection rights at their office door. This means that a country's privacy and data protection laws are likely to apply to workplace monitoring.

- Employers should be clear about the purpose for monitoring and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.

- Any limitation on the employee's rights to privacy should be proportionate to the likely damage to the employer's legitimate interests. Or, conversely, monitoring must be proportionate to the likely damage to the employer's legitimate interests.

- If monitoring is to be used to enforce the organization's rules and standards, make sure that the rules and standards are clearly set out in the policy which also refers to the nature and extent of the associated monitoring. Assure that workers are aware of the policy.

- Workers should be aware of the nature, extent and reasons for monitoring unless there are exceptional circumstances and covert monitoring is justified. In the United States, it is a good practice to ensure transparency employees should be informed about the reasons for monitoring even if such discussion may not be legally required.

- Identify who within the organization can authorize the monitoring of workers and ensure that they are aware of their responsibilities.

- In the European Union, personal data captured during workplace monitoring must be adequate, relevant and not excessive for the purpose for which the monitoring is justified.

- Any monitoring must be carried out in the least intrusive way possible.
- In Europe, the general principles of the Directive apply to all processing of employee personal data, including workplace monitoring.
- Employers must consider if their interests could be adequately protected by traditional measures of supervision.

Best Practice #2: Identify the purposes for monitoring

Identifying the purposes for monitoring is necessary in most of the Key Countries and will almost certainly be required in order to negotiate with employees, works councils and data protection authorities in Europe and elsewhere. Historically, and particularly in the United States, employers have asserted many business reasons to electronically monitor in the workplace, including:

- To monitor employee productivity in the workplace;
- To protect against unauthorized use, disclosure or transfer of personally identifiable information on employees and customers while maximizing the productive use of the employer's computer systems;
- To monitor employee compliance with employer workplace policies related to the use of its computer system, email systems and Internet access;
- To prevent industrial espionage, such as theft of trade secrets and other proprietary information, copyright infringement, patent infringement or trademark infringement by employees and third parties;
- To investigate complaints of employee misconduct, including harassment and discrimination complaints;
- To prevent or respond to unauthorized access to the employer's computer systems including access by computer hackers;
- To protect computer networks from becoming overloaded by large data transfers or denial of service attacks (DDoS);

- To prevent or detect unauthorized utilization of the employer's computer systems for criminal activities and terrorism;

- To help prepare the employer's defense to lawsuits or administrative complaints such as those brought by employees related as to such claims as discrimination, harassment, discipline or termination of employment; and

- To respond to discovery requests in the litigation related to electronic evidence.

A company considering employee monitoring or data loss protection solutions should take the time to understand the company's data flows – what personal or confidential data are used, how and by whom. A data inventory must also identify any sensitive personal information and determine what policies may need to be implemented in order to properly protect such data. The information garnered from the data inventory should be used to demonstrate to management the risks of failing to properly protect data and identify how monitoring and security technology will assist the company in meeting its goals.

The information obtained from an inventory of data flows should also be used to identify the company's greatest areas of risk and then prioritizing them. A company should choose a monitoring, threat detection and data protection technology that can assist in identifying specific risks related to: the users of the data (endpoint), the repository where it's stored (data at rest), the channel of transfers (data in motion) and finally the context or use case of why the data is collected in the first place.

Best Practice #3: Monitoring must be proportionate

In order for an employer to judge whether the monitoring is a proportionate response to the problem that it seeks to address, it must consider a number of factors. In the United Kingdom, the Information Commissioner's Office recommends that this be accomplished by conducting a Data Protection Impact Assessment.[18] In other Key Countries, it may be simply required for the employer to consider certain factors such as:

- Identifying clearly the purposes or uses cases behind the monitoring arrangement and the benefits it is likely to deliver;
- Identifying any likely adverse impact of the monitoring arrangement;
- Considering alternatives to monitor or different ways in which it might be carried out;
- Taking into account the obligations that arise from monitoring; and
- Judging whether monitoring is justified.

Once a company has the information from the Data Protection Impact Assessment, it will be in a position to ensure that the proposed workplace monitoring solution is proportionate to the risks the employer seeks to manage. This information should be documented and available to works councils, trade unions or other representatives of your employees. You may also find that the information in the Data Protection Impact Assessment will facilitate successful discussions with national data protection authorities.

[18] U.K.'s Information Commissioner's Office ("ICO"), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

Best Practice #4: Consultation

It might be tempting to monitor your employees without their knowledge. It may even be warranted. However, many believe that informing employees of monitoring will deter employees from committing malicious or possible criminal activity. It's highly likely that you will get better results if you are open about your monitoring intention and bring your employees onboard from the beginning. From a legal point of view, whether you must engage in such consultation will depend upon a number of factors, including the laws of each Key Country, the size of your company and the existence of any collective bargaining agreements.[19]

It is important for employers to understand the technology they have chosen for monitoring. It is equally important that employers be able to explain to the workers, their unions and other representatives how the monitoring will impact them. Remember that in many countries, workers have the right to participate in decisions that impact the conditions or work. In addition to consulting with the workers and their representatives, it may also be necessary to provide such explanations to the appropriate data protection authorities.

Consultation should include discussion of the following the purposes for monitoring, how monitoring will take place, when it will take place, when it will occur and what will be done with the information collected during the monitoring. If monitoring will involve managing the work habits of employees, then you should be prepared to explain why this cannot be accomplished by means other than automated monitoring. If, however, monitoring is intended to protect company data, employee and customer information or other confidential data, you should be prepared to demonstrate why the use of automated DLP technology is less intrusive than having human intervention. This is particularly important in situations where personal email may be included in information that is subject to monitoring.

[19]Raytheon, "Best Practices for Mitigating and Investigating Insider Threats," https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf.

Best Practice #5: Implement technology that fosters compliance

When making a choice of your company's employee monitoring/UAM/UEBA or DLP solution, you should keep in mind how the technology addresses the privacy and data protection requirements for workplace monitoring and security. The good news is, modern employee monitoring software are designed for such flexibility. These solutions allow customers to effectively monitor the use of confidential information and boost productivity while safeguarding employee privacy. This is accomplished in a number of ways:

- **Compliance with notices and policies** – A solution that supports policy and rules-based monitoring enables companies to comply with their privacy notices and policies. This type of software focuses on data processing that violates company policies vs. capturing everything. They can be configured to record only the relevant sessions and transactions minimizing privacy data capture. Additionally, software such as Teramind comes with pre-built policies and rules for some of the most critical compliance regulations and standards like GDPR, HIPAA, PCI etc. that makes it easy to implement notices and policies required be those laws.

- **Legitimate purposes and proportionality** - Laws like GDPR require that data collected during monitoring is used only for legitimate purposes. In a modern UAM/UEBA/DLP software, this can be achieved in several ways. For example, you can enable or disable certain *objects* like the websites, email, network etc. For example, if you aren't a call center or require it for other solid business reasons, you can disable audio recordings. For objects you've decided to monitor, these software tools allow you to finetune what needs to be captured, how and when to a granular level. Some software, including Teramind even allows dynamic, context-sensitive adjustment of tracking and recording. Such a system can, for example, temporarily suspend monitoring websites when a user visits a banking portal or uses their personal email and turns it back on when the user leaves the session.

- **Access on a need-to-know basis** - This is part of the '*data privacy by design and by default*' principle that enables companies to strengthen data protection by ensuring only those individuals with a "need to know" clearance have access to the collected data. Typically, this is implemented by methods like: identity-based authentication, segregated (or layered) access control and encryption. This way, for example, while an IT administrator can access your HR/CRM database for maintenance purposes, they should not be able to view any unprotected employee or customer data while performing such duties.

- **Targeted monitoring** – Targeted monitoring in this context means, limiting the scope and subject(s) of the monitoring for reasonable purposes. This doesn't mean you should be targeting arbitrary groups - that would be discrimination. However, if you, for example, implement privileged-user rules to protect yourself from threats like unauthorized credential escalation, tampering of critical system resources etc. for your systems administrators and third-parties then that should be a legitimate 'targeted monitoring'. A good employee monitoring software also allows you to focus monitoring based on role functionalities. For example, by monitoring social media usage of your marketing/PR department on your corporate accounts can reduce the cause of privacy violation and still protect your business interests.

- **Data integrity / accuracy** – Collecting information that does not violate policy or information on the wrong individuals increases a company's privacy risks. These risks can be reduced by keeping false positives to a minimum. In addition to applying the above best practices, a solid DLP solution helps you maintain an up-to-date record of the locations and usage of personal information and demonstrate safeguards used to protect the information. The information can be in files, databases, email, unstructured data, backups, DMS, knowledge bases, or anything else that houses data. Immutable session log keeps track of all administrative activities and what action they performed, on which object etc. ensuring data integrity and accuracy;

- **Security** – You can follow security standards like **ISO 27001** or the NIST cybersecurity framework to ensure you have a security perimeter around your organization. However, engaging a third-party solution provider for your employee monitoring or DLP needs can broaden the scope and applicability of such a defense perimeter. The security requirements now have to include your vendor's

platform too. For example, if the employee or customer data collected by the system is kept in the Cloud, you need to know who's responsible for guarding its privacy and security. You should also know if the vendor utilizes security best practices like two/multi-factor authentication, encryption at rest and on the move, disaster recovery etc. and doing their best to protect your customer data. A reputable vendor will have no difficulty clarifying this for you and being transparent about their platform security. If not, walk away from them.

Best Practice #6: Understand the monitoring laws of each country

It is a good chance that one of the states will have similar laws but as you will see in the **Data Protection Law** section, there are variances among the states – even among the Member States of the European Union. To further complicate issues, there just are not a lot of judicial decisions, regulations or legislative guidance in several countries to help guide compliance. This makes it more important for companies operating in these jurisdictions to have a full understanding of the relevant laws and risks. This includes an understanding of the risks of opening employee emails and other forms of communication. Employers who want to monitor must be able to fully comply with the privacy laws and regulations as well as the telecommunication requirements.

The headlines make the point that government officials may impose criminal and/or civil actions for the breach of these requirements. These sanctions may be imposed against individuals as well as organizations. The fines must be effective, proportionate and dissuasive for each individual case and they can be substantial.[20] For the decision of whether and what level of penalty can be assessed, the authorities have a statutory catalogue of criteria which it must consider for their decision. Among other things, the intentional infringement or the failure to take measures to mitigate the damage which occurred, or lack of collaboration with authorities can increase the penalties. For especially severe violations, listed in Art. 83(5) GDPR, the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4% of their total global turnover of the preceding fiscal year, whichever is higher.[21]

[20] See https://gdpr-info.eu/issues/fines-penalties/.

[21] See, InterSoft Consulting, https://gdpr-info.eu/issues/fines-penalties/, for a list of fines that have been imposed so far.

Data Protection Laws

This section provides a detailed overview of the privacy and data protection laws and regulations of leading countries from Australia, Europe, North America and South America, and how they may regulate the implementation of workplace monitoring of DLP. Each jurisdiction is divided into the following sections:

- **Overview** – Provides a brief summary of the privacy and data protection laws;
- **General Privacy Laws** – Identifies the constitutional and statutory provisions for privacy;
- **Personal Data Protection Laws and Regulations** – Identifies significant laws enacted;
- **Workplace Privacy Laws** – Identifies those laws, rules and regulations that may impact an employer's ability to conduct workplace monitoring; and
- **Discussion** – A summary of the key issues related to employee monitoring.

The Member States of the European Union,[22] as well as the European Free Trade Association[23] ("EFTA"), and the other key jurisdictions discussed in this paper, have enacted some of the strictest privacy laws in the world. Additionally, many of these laws specifically regulate the gathering of information in the workplace. The following section examines the efforts of these jurisdictions to effectively balance the interests of all sides of this issue. It is important to understand how these laws may impact a company's ability to implement data loss prevention technology.

[22]Lists of Countries in the European Union, http://worldpopulationreview.com/european-union-countries/ (2019).

[23]European Free Trade Association, www.efta.int.

Oceania

Australia

Overview	Australia regulates data privacy through a combination of federal, state and territory laws. The **Federal Privacy Act 1988**[24] ("Privacy Act") and the **Australian Privacy Principles**[25] apply to private sector entities with an annual turnover of at least AU$3 and all Commonwealth Government and Australian Capital Territory Government agencies.
General Privacy Laws	Under the **Privacy Act**,[26] **Australia's Privacy Commissioner**[27] has the authority to conduct investigations. The law provides employers with the right to monitor employees' computers such as desktops, laptops, servers and their Internet activities. On the whole it is legal to monitor employees' usage of company property. Employers are, however, required to give notice to employees about the monitoring system.

[24] See, https://www.oaic.gov.au/privacy-law/privacy-act/.

[25] See, Australian Privacy Principles, https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles.

[26] Australian Privacy Act. See, https://www.oaic.gov.au/privacy-law/privacy-act/.

[27] Australian Privacy Commissioner.

Personal Data Protection Laws and Regulations

Most states and territories in Australia (except Western Australia and South Australia) have their own data protection legislation applicable to state government agencies, to enforce the Privacy Act and to seek civil penalties for serious privacy violations.

Workplace Privacy Laws

There are dozens of workplace privacy laws across Australia. The following is an overview of some of the laws:

- www.legislation.act.gov.au/a/2014-24/current/pdf/2014-24.pdf[28]
- Health Records and Information Privacy Act 2002 No 71 (Northern Territory).[29]
- Workplace Surveillance Act 2005 - NSW Legislation.[30]
- Privacy and Personal Information Protection Act 1998[31]
- Information Privacy Act 2009 (Northern Territory)[32]
- Information Privacy Act 2009 (Queensland)[33]

[28]See, Information Privacy Act 2014 - ACT Legislation Register.

[29] Privacy and Personal Information Protection Act 1998 (New South Wales).

[30]See, https://www.legislation.nsw.gov.au/inforce/cda3e2c0-0fd3-6065-e243-e81a43c4fdb2/2005-47.pdf

[31]https://www.legislation.nsw.gov.au/#/view/act/1998/133

[32]See, Information Privacy Act 2009, Northern Territory, https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions.

[33]Information Privacy Act 2009 (Queensland).

Australia has other parts of legislation that regulate entities that may regulate specific data such as financial services institutions.

The Workplace Surveillance Act 2005 came into effect on 7 October 2005.[34] This act regulates video surveillance, tracking and computer surveillance including the monitoring of recording of emails and access to Internet websites. Employers are required to comply with both overt and covert rules for surveillance.

Discussion

The **Privacy Commissioner**,[35] under the **Office of the Australian Information Commissioner (OAIC)** is the national data protection regulator. The Commissioner is responsible for Privacy Act oversight.

Australia does not have uniform laws governing the surveillance of employees by private sector employers. Currently, only two jurisdictions in Australia (New South Wales and the Australian Capital Territory) have specific legislation regarding surveillance of electronic communications by employers.

With limited exceptions, computer surveillance by employers of employees in New South Wales[36] is prohibited unless the employee has been given 14 days prior written notice by the employer. The statute requires a written notice of the employer's policies.

[34]See, Workplace Surveillance Act 2005 - NSW Legislation.

[35]Office of the Australian Information Commissioner, https://www.oaic.gov.au/. The Australian Privacy Commissioner has a section on his website entitled "surveillance and monitoring." This section carries information about the latest occurrences on surveillance and monitoring throughout Australia.

[36]See, https://www.legislation.nsw.gov.au/inforce/cda3e2c0-0fd3-6065-e243-e81a43c4fdb2/2005-47.pdf.

Europe

Belgium

Overview

Belgium has a long history of strict data protection laws and compliance.

The **General Data Protection Regulation** (Regulation (EU) 679/2016) (GDPR) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

The application of the GDPR depends on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

The GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behavior*" (Article 3(2)(b)) as far as their behavior takes place within the EU.

The Belgian Data Protection Authority, the successor of the Belgian Privacy Commission, was established by the Belgian Federal Chamber of Representatives by the **Law of 3 December 2017** ("DPA Act").[37]

The general privacy act is the **Act of 8 December 1992** [38] on the Protection of Privacy in relation to the processing of personal data. While Belgian law recognizes the rights of employers to monitor in certain circumstances, their rights are limited, and may require consent of the employees and the relevant works council.

General Privacy Laws

The principle of privacy protection is set forth in **Article 22 of the Belgian Constitution**: "Everyone has the right to respect

[37]On April 25, 2019, the new chairman and the four directors of the new Belgian data protection authority were sworn in before the Belgian Parliament.

[38]See, Act of 8 December 1992 on Privacy Protection.

for his private and family life, except in the cases and under the conditions stipulated by law."[39]

The right to privacy is directly binding and can be enforced by employees in the labor courts. The law recognizes several exceptions, many of which are the result of making the employer liable for the damages caused by the employee in the execution of their employment contract. Generally, employers can take actions to control how and when technology, including e-mail, can be used.

Personal Data Protection Laws and Regulations

Belgium enacted the **Act of 8 December 1992**[40] on the protection of privacy in relation to the processing of personal data (BDPA). The BDPA ensures that the personal data may only be processed for clearly described and justified purposes and may not be used in a manner incompatible with these purposes. The Act applies: (a) when the processor is carried out in the context of activities of a permanent establishment of the controller in Belgium; or (b) if the controller, established outside the EU makes use of equipment located in Belgium, except for mere transit.

Workplace Privacy Laws

The **Belgian Law of 30 July 2018**[41] on the protection of natural persons with regard to the processing of personal data (**Law of 30 July 2018**) entered into force on 5 September 2018. This

[39]Belgian Constitution of 1831 with Amendments Through 2014.

[40]Legislation relates to the protection of privacy in relation to the processing of personal data (BDPA).

[41]Tom De Cordier and Thomas Dubulsson, "New Belgian Data Law Comes in Force," Lexology, https://www.lexology.com/library/detail.aspx?g=62bedd62-050c-4b78-8996-987b8142f718.

piece of legislation abolishes the Law of 8 December 1992 on privacy protection on privacy protection when processing personal data (Law of 1992) which regulated the processing of personal data in Belgium for almost 26 years.

The Belgian Law of 30 July 2018 brings to a logical end the coexistence of 1992 and the EU General Data Protection Regulation 2016/679 ("GDPR"). The GDPR came into force on 25 May 2018 and directly applies to data processing activities performed by Belgium-based controllers and processors. After the Law of 3 December 2017 creating the Data Protection Authority (replacing the Commission for the Protection of Privacy), tasked with the monitoring compliance with their privacy obligations, the Law of 30 July 2018 is the second piece of Belgian legislation triggered by the GDPR.

The entry into force of the Law of 30 July 2018 is unlikely to have a significant impact on companies processing personal data.

However, the Law of 30 July 2018 impacts organizations relying consent from children or processing special categories of data. The Belgian legislator set 13 as the age from which children may provide consent of an information service, lower than the age of 16 set by GDPR.

Royal Decree of 13 February 2001 [42]

Workplace monitoring is governed by at least seven different legal documents from different fields of law. For example, **Collective Bargaining Agreement No. 81**, the **Royal Decree**

[42]Royal Decree, 13 February 2001 implementing the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data Unofficial translation – September 2008.

of 13 February 2001, the **Data Protection Act**, Section 124 of the **Electronic Communications Act** (unauthorized access to electronic communications) and 314 *bis* of the **Criminal Code** (unauthorized tapping during the transmission). The interplay of these legal documents is explained by the Privacy Commission in report.

Article 2, §1 of the **Collective Bargaining Agreement No 13 December 1983** provides that "once an employer has decided to invest in new technology which has important collective consequences . . . working conditions, he must before the beginning of the introduction of the new technology provide information about the nature of the new technology, about the factors that justify its introduction and its consequences and consult with the representative of the employees on the introduction of the new technology."

Belgian law imposes restrictions on monitoring employees.[43]

Employers can monitor the use of e-mail and the Internet during working hours provided that a number of conditions are met as follows:

- The monitoring should serve as one of the purposes defined by the agreement. These purposes are limited by CBA No 81;
- The prevention of wrongful or defamatory acts;
- The protection of the company's economic and financial interests;

[43]The conditions are negotiated.

- The security and proper functioning of the company's IT network;
- Ensuring employees compliance with the company's IT policy;
- The monitoring should be proportional to its purposes;
- Prior to implementing the monitoring, all employees concerned should be informed collectively (through their representative bodies) and individually of the fact that monitoring may occur and for what purposes.

Discussion

Do employees have access to data held about them and if so, what rules apply? In execution of Article 10 of the Privacy Act any data subject has the right to obtain from the controller:

- Information on whether or not data remaining to him is being processed as well as what information regarding the purposes of the processing, the categories of data the processing relates to and the categories of recipients the data is disclosed to; to and
- Communication of the data being processed in an intelligible form, as well as of any available source information. To obtain the information the data subject must submit a signed and dated request to the controller who shall communicate the information without delay, or at the very latest forty-five days after receipt of the request.

France

Overview	The **French Data Protection Authority** ("CNIL") is one of the largest data authorities in Europe and actively enforces the French privacy and data protection laws.[44] The **French Labor Code**[45] recognizes the employer's right to monitor the property performance of work tasks by its employees, provided that such monitoring does not violate the employee's fundamental rights and freedoms. (Art. L 120-122). Network Monitoring of employees is thus permitted, subject to the protection of the employees' rights.
General Privacy Laws	**Article 9 of the French Civil Code** provides that willfully infringing someone else's privacy rights is a criminal offense and specifies penalties incurred for interception of correspondence.
Personal Data Protection Laws and Regulations	**Act. No. 78-17 Amended by the Act of 6 August 2004** relating to the Protection of Individuals with regard to the Processing of Personal Data.

[44] www.cnil.fr.

[45] The New French Labor Code; https://lawnn.com/labour-law-france-new-french-labour-code/.

Workplace Privacy Laws

In France, the Labor Code recognizes the employer's right to monitor the performance of work tasks by its employees. Provided that such monitoring does not violate the employee's fundamental rights and freedoms. (Art. L120-2). Network monitoring of employees is thus permitted subject to the protection of the employees' rights.

French law discusses when monitoring is justified. If the company has reason to believe that, in view of the duties and responsibilities held by an employee, he or she could potentially undermine the integrity of the computer systems or otherwise act against the company such as by making it vulnerable to a security breach affecting confidential data, inflicting damage on the computer systems, causing technical disruptions or exposing it to the risk of incurring liability toward third parties as a result of a data transfer, then monitoring is justified. (Labor Code Art. L. 120-2).

In October 2001, France's highest appellate court held in ***Nikon France v. Onos*** that employers do not have the right to read their employees' personal e-mail or other personal computer files stored on a work computer. Since 2006, however, the courts have determined that e-mails and files stored on a company's network are presumed to be work-related, except if they are clearly flagged as "personal" or "private."

On 21 October 2009, in Decision No. 07-43877, the French Supreme Court ruled that files created by an employee on a computer issued by his employer for work purposes were presumed to be professional unless the employee identified them clearly as personal. If the employee has clearly identified the files as personal, the employer has to either obtain the employee's prior consent before opening the files or to go

before a court to obtain an order allowing the employee to open the files.

Discussion

French law specifically applies the **principle of proportionality**: workplace monitoring is justified only if it is necessary to protect the legitimate business needs of the employer and goes no further than is necessary to meet that need.

Companies operating in France should examine their policies and practices conveying monitoring of computer files and electronic communications and carefully tailor and limit monitoring to protect identified and legitimate business interests.

Then, in 2010, a new data-privacy case decided by the French Cour de Casson (high court), called **Bruno B v. Giraud et Migot**, Cour de Cassation [Cass.], soc., Paris, 15 Dec. 2009, No. 07-44264. Bruno B was "a significant development" because, previously, French privacy laws offered an extremely high level of protection for employees' data, as exemplified by the 2001 decision, Nikon France v. Onos, Cour de Cassation [Cass.], soc., 2 Oct. 2001, No. 4164.

Germany

Overview

Data processing in Germany is generally governed by the **Federal Data Protection Act 2002** ("FDPA") and by the federal constitution. The FDPA applies to all types of data processing activities that are carried out in Germany, including those in the workplace.

According to many, Germany is generally regarded as having the strictest data protection laws in the world. These laws are vigorously enforced and fines are substantial.

General Privacy Laws

Article 10 of the Basic Law [46] (the German Constitution) provides protections for letters, posts and communications.

Personal Data Protection Laws and Regulations

The FDPA implements the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Personal Data and on the free movement of such data (EU Data Protection Directive).

The law applies to data controllers located in Germany or to those located outside Germany but processing personal data in Germany.

[46] See, Basic Law of German Constitution, see, https://www.gesetze.im-internet.l.de/englisch-rr.

Workplace Privacy Laws

The **Works Constitution Act**[47] gives works councils co-determination rights over: rules of conduct where the employer permits the use of company's e-mail for private purposes; and introduction and use of technical equipment intended to monitor conduct or performance of employees.

For job-related e-mails, under Section 4.28 para. 1 nos. 1 and 2 of the Federal Data Protection Act, monitoring is permissible if (a) it is required for purposes of carrying out the employment contract; (b) justified by prevailing interest of the employer. Consent from the employee is not required.

For job-related e-mails, the employer can monitor information about the sender, recipient, time, date, data volume, etc. The employer is also entitled to monitor content of such e-mails. However, the employer may not check all e-mails of an employee in order to control the employee's performance. If private e-mails are detected, the employer should disregard them once it is detected that they are private.

If the employer allows private e-mails, then the employer may be regarded as a telecommunications service provider under the provisions of the **Telecommunications Act of 22 June 2004**.[48] In such a situation the employer would not be allowed to monitor private e-mails. Any information gathered from such private e-mails could only be used for providing services.

Discussion

In August 2010, the German Government proposed amendments to German law regarding employee data

[47]See, Works Constitution Act (2001) http://www.gesetze-im-internet.de/englisch_betrvg/.

[48]Telecommunications Act of 22 June 2004; See, https://rm.coe.int/16806af19e.

protection. The amendments, however, have not been enacted nor have they been clarified whether an employer that allows private use of its e-mail system is to be classified as a "telecommunications provider" and as such, subject to telecommunications secrecy. The amendments would also distinguish between work related e-mails that have completed transmission and those that have not completed transmission. The employer must still give written notice to employees before viewing e-mails.

Italy

Overview	The Garante per la Protezione dei Dati Personali ("Italian Data Protection Authority") has aggressively enforced the Italian data protection laws.[49] On 1 March 2007, the Italian Data Protection Authority issued the **Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context**.[50]
General Privacy Laws	Although the Italian Constitution has several limited provisions related to privacy, none specifically apply to the workplace.
Personal Data Protection Laws and Regulations	The **Italian Personal Data Protection Code** has several limited provisions related to privacy; none specifically apply to the workplace.
Workplace Privacy Laws	The **Italian Data Protection Code** brings together all of the various laws, codes and regulations relating to data protection since 1996. The Code implements parts of the E-Communications Privacy Directive (see Title 10, Part 2 of the

[49]See, https://www.garanteprivacy.it/home_en.

[50]See, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1665291.

Code). Section 115 of the Code relates to the protection of home-based or "teleworkers." The Code requires employers to ensure that the employees' personality and moral freedom are respected. Additionally, the Code provides "Home-based workers shall be required to ensure confidentiality as necessary with regard to all family-related matters."

Legge No. 93 of 29 March 1983,[51] applies to workplace monitoring but does not prohibit employer's rights in this area.

Article 4 of the **Workers' Statute (Law No. 300/1970)** [52] prohibits the use of new technologies to control workers' activities - although this does not prohibit workplace monitoring. Under this statute, employers are prohibited from investigating political, religious or trade unions opinions of workers. The Italian Data Protection Authority has drawn a distinction between workplace monitoring for purposes of controlling employees and "defensive" monitoring.

On 1 March 2007, the Italian Data Protection Authority issued the **Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context.**[53]

The Italian Supreme Court upheld a ruling in favor of an employer who determined that an employee was improperly using customer information in an e-mail. The employee contested his dismissal arguing that e-mail monitoring violated **Section 4** of the **Italian Statute of Workers' Rights (Law 300/1970)**. The Supreme Court noted, however, that this

[51] Legge No. 93 of 29 March 1983.

[52] See, https://www.eurofound.europa.eu/efemiredictionary/workers-statute.

[53] See, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1408680.

implies that employees are engaged only in legitimate activity. The Court confirmed that "defensive monitoring" is not covered by Section 4.

According to the Italian Supreme Court, "defensive monitoring" refers to controls that are legitimately put in place to protect company assets and/or to detect illegal conduct on the part of employees and, therefore, falls outside of Section 4. Defensive monitoring is intended to detect wrongful conduct that may harm the employer's assets. In these circumstances, the employer's right to protect its assets and images prevails over the employee's rights to privacy.

It is unclear how the Supreme Court's decision will impact the Data Protection Authority's Guidelines applying to the extent possible, limit monitoring to "defensive monitoring" and comply with the binding principles set forth in the guidelines. This would include giving notice, publishing appropriate policies and guidelines and obtaining approval by works councils or labor administration department. The data protection principles set forth in the guidelines are:

1. Necessity;
2. Finality;
3. Transparency
4. Legitimacy;
5. Proportionality;
6. Accuracy and Retention;
7. Security.

In addition, companies should have a legitimate purpose for monitoring.

Discussion

Employers should adopt a policy describing the monitoring that will take place and describing the purpose for monitoring. Monitoring should be targeted to communications that violate specific policies. Use of the data should be limited and the data appropriately secured. The notice of monitoring must include the following:

1. the conditions for using Internet and e-mail at work;
2. the extent to which private use of the Internet and e-mail is accepted in the workplace;
3. the fact that e-mails may be monitored and the specific purposes for monitoring;
4. what kind of information can be stored temporarily and who is authorized to have access to it;
5. the options to be used in the event of an employee's absence;
6. the security measures in place;
7. the modalities of the monitoring activities; and
8. the applicable sanctions in case of abuse and the ways in which employees can exercise their rights.

Employers should implement policies regarding retention of data and must ensure that employee data are periodically deleted for appropriate reasons.

Italian law provides for criminal and civil penalties. Additionally, the **Italian Civil Code, Art. 2050**, also permits recovery of damages.

Spain

Overview

The **Spanish Data Protective Act (Organic Law 15/1999)**[54] is an omnibus act. Spain's Data Protective Commissioner is active in enforcing private rights. Spain has a number of laws protecting personal privacy. It also has a number of courts that hear labor disputes:

- Labor Courts
- Labor Chamber of the High Court of Justice
- Labor Chamber of the National High Court
- Labor Chamber of the Supreme Court (all of the judges are magistrates).

General Privacy Laws

Article 8 of the Spanish Constitution provides the right to personal and family privacy.

Article 167 of the Spanish Penal Code prohibits the unlawful interception of communications.

Note, however, that neither of these explicitly applies to workplace monitoring.

[54]Spanish Data Protective Data Act (Organic Law 151/1999).

Personal Data Protection Laws and Regulations

Royal Decree 1720/2007 of 21 December, which approves the regulation implementing Organic Law 15/1999, of 13 December on the protection of personal data.

Organic Law 15/1999 of 13 December on the Protection of Personal Property.

Royal Decree 994/1999 of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data.

Act 34/2002 of 11 July on Information Society Services and Electronic Commerce. Extract of relevant articles regarding personal data protection.

Act 41/2002, of 14 November 2002, basic regulating Act on the autonomy of the patient and on the rights and obligations in matters of clinical information and documentation.

Article 32/2003 (State Telecommunications Act).

Workplace Privacy Laws

Article 64 of the Workers' Statute established the right of works councils to issue a report on the introduction of monitoring.

Articles 5 and 20 of the Labor Act give employers the right to direct the labor activity and to monitor or supervise employees' work-related obligation – but these rights must not impinge the dignity of the workers.

Discussion

Spain has approved the **Organic Law on the Protection of Personal Data and Guarantee of Digital Rights** ("LOPD")

which adapts national legislation to the General Regulation on Data Protection of the European Union. The LOPD establishes new labor rights and obligations for employers in its Title X "Guarantees of digital rights". These rights include:

- **Right to privacy in the use of digital devices:** Employees shall have the right to the protection of their privacy in the use of the digital devices their employer makes available to them (art. 87 LOPD).
- **Right to digital disconnection:** Employees have the right to "digital disconnection". This means that employees can turn off digital devices outside working hours, being unreachable. (art. 88 LOPD).
- **Right to privacy from the use of video surveillance and sound recording devices in the workplace:** Images obtained by camera systems or video cameras to control employees may be processed by employers, provided that certain legal requirements and limits are respected. Systems for the recording of sounds will only be admitted for safety purposes and always respecting certain principles. (art. 89 LOPD).
- **Right to privacy in case of geolocation system use:** The data obtained through GPS systems may be processed by employers for the exercise of control functions, provided they are exercised within their corresponding legal framework. Employees must be informed about the existence of such devices. Employees must also be informed about the possible exercise of rights of access, rectification, limitation of treatment and deletion (art. 90 LOPD).
- **Digital rights in collective bargaining:** Collective bargaining may establish additional guarantees in relation to the processing of personal data and the safeguarding of digital rights (art. 91 LOPD).

United Kingdom

Overview	The United Kingdom has an active Information Commissioner's Office with a large staff, but the Commissioner has limited enforcement powers.
General Privacy Laws	The **Data Protection Act of 1998** implemented the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of personal data and on the free movement of such data (EU Data Protection Directive).
Personal Data Protection Laws and Regulations	The **Regulation of Investigatory Powers Act of 2000 ("RIP")**[55] regulates the monitoring or interception of e-mails and other forms of communication. The Telecommunications (Lawful Business Practice) (Interception of Communication Act) Regulation 2000 also regulates the interception of communications including e-mails.

[55]Regulation of Investigatory Powers Act of 2000, http://www.legislation.gov.uk/ukpga/2000/23/contents.

Workplace Privacy Laws

The **UK Information Commissioner**[56] has provided extensive guidance, including the **Employment Practices Code Supplemental Guidelines**[57]

The Code and Guidelines set forth specific requirements and procedures that must be followed before monitoring can take place. For example, a Privacy Impact Assessment must be performed before monitoring takes place. This should document the business need for monitoring, and the method of monitoring must be targeted and the least intrusive possible. Written notice must be provided to employees providing clear information on how monitoring will be conducted, what information will be collected and the reason for the monitoring.

Discussion

The UK Information Commissioner's **Employment Practices Code** and **Employment Practices Code: Supplemental Guidance** discuss steps that companies must follow if they are to engage in workplace monitoring:

1. Conduct the assessment required by the Code;
2. Adopt and publish a policy and notices that are known and understood by the workers;
3. Follow the rule of proportionality and minimize the monitoring of target actions that violate specific policies;
4. Limit the access to monitored information to only those who have a need to know;

[56]Information Commissioner's Office; https://ico.org.uk/.

[57]Employment Practices Code, https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf.

5. Ensure that information is kept securely and not improperly disclosed;

6. Comply with the requirements of the Data Protection Act, the Lawful Business Practices Regulations, and the Code and Guidelines;

7. Use sophisticated automated monitoring systems to assist data protection compliance. In addition, businesses should ensure that employees continue to have secure lines of communication for the transmission of sensitive information from workers to a health provider or for trade union communications that will not be monitored.

The Information Commissioner seems to draw a distinction between surveillance where human "open" e-mails or other communications and the use of monitoring technology to determine if the content of an e-mail violates policy. The Information Commissioner has suggested that companies consider monitoring to implement appropriate technologies that can assist in compliance.

North America

Canada

Overview

In Canada, there are numerous laws that relate to privacy rights. The principal law is the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, which became law on 13 April 2000 and came into full effect on 1 January 2004 after a two-stage implementation. The legislation not only covers the ways data should be safely stored in the digital world, but also how organizations must collect, use and disclose personal information in the course of commercial activities. It is significant to note that PIPEDA applies only to federally-regulated organizations.

There are also sector-specific laws such as the health-related laws and the financial services.

General Privacy Laws

Personal Information Protection and Electronic Documents Act [58]

Every province and territory has its own privacy-related laws. Some sector-specific laws have been deemed "substantially

[58] See, Personal Information Protection and Electronic Documents Act, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

similar" to PIEPEA which means those laws apply instead of PIPEDA in the following provinces:

- Alberta
- British Columbia
- Quebec

The following provinces have health-related privacy laws that have been declared substantially similar to PIPEDA:

- Ontario
- New Brunswick
- Newfoundland
- Labrador
- Nova Scotia

Personal Data Protection Laws and Regulations

PIPEDA does not apply to:

- Not-for-profit and charity groups
- Political parties and charity groups
- Political parties and associations
- Municipalities, universities, schools and hospitals

PIPEDA does not apply to organizations that operate entirely within:

- Alberta
- British Columbia
- Quebec
- Federally-regulated businesses

PIPEDA generally applies to personal information held by private sector organizations that are not federally-regulated, and conduct business in:

- Manitoba
- New Brunswick
- Newfoundland and Labrador

- Northwest Territories
- Nova Scotia
- Nunavut
- Ontario
- Prince Edward Island
- Saskatchewan
- Yukon

Workplace Privacy Laws

Some provinces have passed privacy laws that apply to employee information:

- Alberta
- British Columbia

Discussion

Each province and territory in Canada has a commissioner or ombudsman responsible for overseeing provisional and territorial private legislation.

PIPEDA Fair Information Principles:

- Principle 1: Accountability;
- Principle 2: Identifying Purpose;
- Principle 3: Consent;
- Principle 4: Limited collection;
- Principle 5: Limiting Use, Disclosure and Retention;
- Principle 6: Accuracy;
- Principle 7: Safeguards;
- Principle 8: Openness;
- Principle 9: Individual Access; and
- Principle 10: Challenging Compliance.

Mexico

Overview

The National Institute of Transparency for Access to Information and Personal Data Protection. (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) (INAI) and the Ministry of Economy (*Secretaría de Economía*) serve as Mexico's data protection authorities.

The National Institute for Transparency, access to Information and Personal Data Protection (INAI) is an autonomous constitutional body responsible for upholding the right to access to public information held by any authority, entity, body or agency belonging to the executive, legislative and judicial branches, as well as by any individual, moral person or labor union that receives and spends public money or performs acts of authority at the federal level. The INAI is also in charge of upholding the right to protection of personal data held by the public and the private sectors.

The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Proteccion de Datos Personality en Possession de los Particulares) entered into force on 6 July 2010).

General Privacy Laws

The Executive Branch has issued the following:

- The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties.[59]
- The Privacy Notice Guidelines which entered into force on 18 April 2013.
- The recommendations on Personal Data Security on 30 November 2013.
- The Parameters for Self-Regulation regarding personal data which entered into force on 30 May 2014.
- The General Law for the Protection of Personal Data for Possession of Obligated Subjects which came into force on 27 January 2017.

As of 2009 protection of personal data was recognized in the Mexican Constitution as a fundamental right.

The Mexican laws applies primarily to companies located in Mexico, but in some cases also to non-Mexican companies doing business in Mexico.

Personal Data Protection Laws and Regulations

On 12 June 2018, a decree was published in the Official Gazette of the Federation approving two important documents: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated 28 January 1981, and its Additional Protocol regarding supervisory authorities and trans-border data flows dated 8 November 2001.

[59] See, http://inicio.ifai.org.mx/English/2%20Regulations%20to%20the%20FLPPDHPP.pdf.

Workplace Privacy Laws

The processing and use of personal data are subject to certain basic principles set out in the Data Protection Law

When personal data is to be collected individuals must be provided with his privacy notice that must contain the following information as a minimum:

- The identity and address of the data controller;
- The purposes on the processing of the personal data;
- The available options and resources that the data controller offer;
- Details of any transfer of personal data that have been carried out;
- The procedure and resources through which the data controller can communicate to the individual any change in the privacy notice;.

The individual would then have the right to access, correct, oppose the processing or use of, and cancel/delete their personal data except as otherwise established by law.

Discussion

The law has requirements for providing notice of breach to the individual.

United States

Overview

In the United States, employers are generally allowed to monitor employees' activities, workstations and almost any aspect of employees' activities on a computer or workstation. Courts generally determine that since the employer owns the computer, network, workstations and the terminals, they are free to use them.

Employers are motivated by concern over litigation and the increasing role that electronic evidence plays in lawsuits and government agency investigations.[60] Such monitoring is virtually unregulated. Therefore, unless company policy specifically states otherwise, your employer can monitor most of your workplace activity. These policies may be communicated through employee handbooks by memos, in union contracts, and by other means. Courts have generally found that when employees are on the job, their expectation of privacy is limited. Employers are generally allowed to monitor your activity on a workplace computer or workstations. Since the employer owns the computer network and the terminals, he or she is free to use them to monitor employees.

If an email or instant messaging system is used at a company, the employer owns it and is allowed to review its contents. Messages sent within the company, as well as those that are sent or received to or from another person's or company can be

[60]See, Privacy Rights Clearinghouse, "Workplace and Privacy and Employee Monitoring," (March 25, 2019) https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring.

subject to monitoring by your employer. Employees should assume that their email and instant messaging on a company system is being monitored and is not private.

In most instances, your employer may monitor your use of any employer-provided mobile phone or device.

Generally, employers may open mail addressed to you at your workplace. Although federal law prohibits mail obstruction, mail is considered delivered when it reaches the workplace.

Employers may monitor employees' use of any employer-provided mobile phone or device.

Employers may use Global Positioning Systems (GPS) devices to track employees in employer-owned vehicles.

General Privacy Laws

State-level momentum for comprehensive privacy bills is at an all-time high. After the **California Consumer Privacy Act**[61] passed in 2018, multiple states proposed similar legislation to protect consumers in their states. Another 13 states are considering similar legislation.
These states include, Hawaii, Maryland, Massachusetts, Mississippi and New Mexico.[62]

[61]See, https://www.oag.ca.gov/privacy/ccpa.

[62]See, "State Law Development in Consumer Privacy," National Law Review (March 15, 2019) https://www.natlawreview.com/article/state-law-developments-consumer-privacy.

Personal Data Protection Laws and Regulations

Employers have the right to monitor the employees' use of computers, such as desktops, laptops and servers and their Internet activities.

Local legislation varies, but depending on the state, it is generally legal for a company to monitor the usage of its own property, including but not limited to computers, laptops and cell phones.

However, every state has its local regulations as to the issue of employee monitoring legacy. For example, certain states require that employers provide notice to their employees before doing so, and several states have pending legislation that would require prior notice.

Specifically, Connecticut and Delaware currently have laws requiring employers to provide notice before conducting electronic monitoring, and New York, Massachusetts, and Pennsylvania all have legislation pending that would require notice before conducting electronic monitoring. (Connecticut General Statute § 31-48d; The Delaware Statute § 705; The Massachusetts Bill § 3(a)-(b); The Pennsylvania's Statute § 2(b); A. 3871, 2009-2010, Reg. Sess. N.Y. 2009).[63]

Workplace Privacy Laws

According to the **Federal Electronic Communications Privacy Act "(ECPA)"** an employer-provided computer system is the property of the employer. Employers that provide employees with a computer system and Internet access are free

[63]Worktime, "USA Employee Monitoring Laws: Are Employees Allowed to Monitor Employee Persona email Messages," (February 17, 2019) https://www.worktime.com/usa-employee-monitoring-laws-are-employers-allowed-to-monitor-employee-personal-emails-messages.

to monitor almost everything employees do with the computer and Internet access which employees have been provided.

Federal Electronic Communications Privacy Act, 18 U.S.C. Section 2511.

Discussion

Electronic Communications Storage Act,[64] **18 USC Section 1030**, and state laws generally make it illegal for employers to intercept private e-mail or to use employees' personal logon and password in order to notify employees that their e-mail is being monitored.

USA has expansive rights for employer to listen to employees' calls at work. Employers may monitor calls with clients or customers for reasons of quality control. In California, however, when the parties to the call are all in California, state law requires that they be informed that the phone call is recorded or monitored by putting a beep tone on the line or playing a recorded message.[65]

[64] See, Electronic Communications Privacy Act of 1986. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

[65] Privacyrights.org, "Workplace Privacy and Employee Monitoring," (https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring) (March 25, 2019).

South America

Argentina

Overview

In 2003, Argentina became the fourth country, only after Switzerland, Hungary and Canada, to be considered for "adequate protection" under the EU standards. For a number of years, it was the only Latin American country with a comprehensive data privacy law.

Argentina received the adequacy determination from the European Union Commission.[66] The determination documents Argentina's measures to protect personal data within the country.

The **Constitution of Argentina** is the basic governing document of Argentina, and the primary source of existing law in Argentina.[67]

Article 43 of the Federal Constitution, third paragraph, provides, in relevant part that any person may file an action to have access to personal data about such person and to information about the purpose with which they are kept, included in public data registries or banks, or in private data registries or banks, and to request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory.

[66]See, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490.

[67]The Constitution is available at http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf.

These provisions do not create an express constitutional right to privacy or data protection, but they do create the basic framework for the protection of such right, as well as the foundation for the legislation, subsequently enacted, which regulates the details of that protection.

Law 25,326 - the Personal Data Protection Law (PDPL) includes the basic personal data rules. It follows international standards, and has been considered as granting adequate protection by the European Commission. **Decree 1558 of 2001** includes regulations issued under the PDPL. Further regulations have been issued by the relevant agencies.

The **Argentine National Constitution**[68] is made up of the following:

- Personal Data Protection Law 25, 326 (PDPR);
- Regulatory Decree 1558/2001 (DP Decree);
- Provisions issued by the National Directorate for Personal Data Protection (INDPDR);
- The Argentine Data Protection Regulation protects all types of personal data.

General Privacy Laws

Article 43 of the Federal Constitution provides that any person may file an action to have access to personal data about such person and to information about the purpose with which they are kept, included in public data registries or banks, or in private data registries or banks, and to request the suppression,

[68] Argentina Constitution; see, www.biblioteca.jus.gov.ar/argentina-constitution.pdf.

correction, confidentiality or updating of the data where inaccurate or discriminatory.

These provisions do not create an express constitutional right to privacy or data protection, but they do create the basic framework for the protection of such right, as well as the foundation for the legislation, subsequently enacted, which regulates the details of that protection.

Law 25,326 - the Personal Data Protection Law (PDPL) includes the basic personal data rules. It follows international standards and has been considered as granting adequate protection by the European Commission. Decree 1558 of 2001 includes regulations issued under the PDPL. Further regulations have been issued by the relevant agencies.

Personal Data Protection Laws and Regulations

Argentina Law 25326 is recognized as providing "adequate protection" under the privacy laws of the EU.

Workplace Privacy Laws

Argentina was the first Latin American country to enact comprehensive EU-style data protection laws. In 2003, Argentina became the fourth country, only after Switzerland, Hungary and Canada to be considered an "adequate protection" jurisdiction.

Discussion

There is legislation in Argentina according to which employers have the right to keep track on company's property, but not employees' personal devices. Based on this, every employee has the right to personal privacy.

Although no case has addressed the applicability of the Personal Data Act to the monitoring of email and Internet use, there are cases which suggest that the monitoring of email and Internet use may be considered the processing of personal data under the Act and, therefore, regulated under the Act. Accordingly, if the employer does not comply with the Act when monitoring employees' emails and Internet use, liability will arise.[69]

[69]Worktime, "Argentine Employee Monitoring Laws: What are Employers Allowed and Not Allowed Doing in the Workplace," https://www.worktime.com/argentine-employee-monitoring-laws-what-can-and-cant-employers-do-in-the-workplace. (2018).

Brazil

Overview

Brazil recently enacted the Brazilian General Data Program, which has decided to invest in new technology which has important collective consequences section Law (LGPD), Federal Law No. 13,709/2018, which was published on 15 August 2018. The LGPD is Brazil's first comprehensive data protection regulation and it is largely aligned to the EU General Data Protection Act (GDPR).

On 28 December 2018, the Provision Measure No. 869/2018 was published, which amended certain LGPD provisions and created the **National Data Protection Authority (ANPD)**. Among other modifications, the LGPD will go into full force in August 2020, rather than February 2020 as required when the LGPD was first published. The LPGD, as amended, will take effect in August 2020.

Prior to the LGPD, data privacy regulations in Brazil consisted of various provisions spread across Brazilian legislation. For example, Federal Law No. 12,965/2014 and its regulating Decree No. 8,771/16 (together, the **"Brazilian Internet Act"**), which imposes some requirements regarding security and the processing of personal data and other obligations on service providers, networks and applications providers, as well as rights of Internet users.

General provisions and principles applicable to data protection are also found in:

- The Federal Constitution;
- The Brazilian Civil Code;
- Laws and regulations that address;
- Particular types of relationships (*e.g.*, Consumer Protection Code and employment laws);
- Particular sectors (*e.g.*, financial institutions, health industry, or telecommunications); and
- Particular professional activities (*e.g.*, medicine and law),

Additionally, there are laws on the treatment and safeguarding of documents and information handled by governmental entities and public bodies.

The LGPD applies to any processing operation carried out by a natural person or a legal entity, of public or private law, irrespective of the means used for the processing, the country in which its headquarter is located or the country where the data are located, provided that:

- The processing operation is carried out in Brazil;
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil; or
- The personal data was collected in Brazil.

On the other hand, the law does not apply to the processing of personal data which is:

- Carried out by a natural person exclusively for private and non-economic purposes;
- Performed for journalistic, artistic or academic purposes;
- Carried out for purposes of public safety, national security and defense or activities of investigation and prosecution of criminal offenses (which will be the subject of a specific law); or
- Originated outside the Brazilian territory and are not the object of communication;
- Shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, provided that the country of origin offers a level of personal data protection adequate to that established in the Brazilian law.

Due to a broad interpretation established in case law in Brazil, practically every Internet user is considered a 'consumer' for consumer protection purposes.

General Privacy Laws

The **Brazilian General Data Program** was published 15 August 2018. The National Data Protection Authority will be published in 2020.

Personal Data Protection Laws and Regulations

The LPGD goes into effect in August 2020.

Workplace Privacy Laws

Brazil's Senate Passed General Data Protection Law
Posted on 11 July 2018. On 10 July 2018, Brazil's Federal Senate approved a **Data Protection Bill of Law** (the "Bill"). The Bill, which was inspired by the EU General Data Protection Regulation ("GDPR").

The Bill establishes a comprehensive data protection regime in Brazil and imposes detailed rules for the collection, use, processing and storage of personal data, both electronic and physical.

Key requirements of the Bill include:

National Data Protection Authority. The Bill calls for the establishment of a national data protection authority which will be responsible for regulating data protection, supervising compliance with the Bill and enforcing sanctions.

Data Protection Officer. The Bill requires businesses to appoint a data protection officer.

Legal Basis for Data Processing. Similar to the GDPR, the Bill provides that the processing of personal data may only be carried out where there is a legal basis for the processing, which may include, among other bases, where the processing is:

1. done with the consent of the data subject;
2. necessary for compliance with a legal or regulatory obligation;
3. necessary for the fulfillment of an agreement; or
4. necessary to meet the legitimate interest of the data controller; or third parties. The legal basis for data processing must be registered and documented. Processing of sensitive data (including, among other data

elements, health information, biometric information and genetic data) is subject to additional restrictions.

Consent Requirements. Where consent of the data subject is relied upon for processing personal data, consent must be provided in advance and must be free, informed and unequivocal, and provided for a specific purpose. Data subjects may revoke consent at any time.

Data Breach Notification. The Bill requires notification of data breaches to the data protection authority and, in some circumstances, to affected data subjects.

Privacy by Design and Privacy Impact Assessments. The Bill requires organizations to adopt data protection measures as part of the creation of new products or technologies. The data protection authority will be empowered to require a privacy impact assessment in certain circumstances.

Data Transfer Restrictions. The Bill places restrictions on cross-border transfers of personal data. Such transfers are allowed (1) to countries deemed by the data protection authority to provide an adequate level of data protection, and (2) where effectuated using standard contractual clauses or other mechanisms approved by the data protection authority.

Noncompliance with the Bill can result in fines of up to two percent of gross sales, limited to 50 million reias (approximately USD 12.9 million) per violation. The Bill will take effect 18 months after it is published in Brazil's Federal Gazette.

Discussion

The Bill was signed into law in mid-August and is expected to take effect in early 2020.

Chile

Overview

Personal data protection is regulated by different laws. The constitution is the Constitution of 1980, Amended to 2012.[70] The laws related to privacy is generally found in the Article 19, No. 4 and No. 5 of the Constitution regarding the right to "respect and the protection of private life" and the "inviolability of the home and every way of private communication."

Criticism of the lack of protections for personal data.

There is no explicit constitutional protection for privacy.

The **Law No. 19.628** of personal data in general regulates the protection concerning natural persons which are considered owners of data.

General Privacy Laws

In 1999, Chile became the first South American country to pass a comprehensive data law. Critics argue that the law is weak as it does not grant data the same protected status as "private life" or "private communication."

Chile has no data protection authority.

There are numerous areas of the jurisprudence that relate to privacy in regard to specific subjects. Here is a partial list:

[70]Constitution of 1980 amended to 2012., See, https://www.constituteproject.org/constitution/Chile_2012.pdf.

1. Privacy in Telecommunications. **Law No. 18.168**. These generally regulate the use of the radio, the telephony, the television and the Internet, services characterized by distance of communications. In Chile, Law. No. 18.168 regulates every transmission, broadcast or signal, documents, image, sounds or information of any nature, by physical line, radio electricity, optical means or other electromagnetic systems, considering regulation is on the intercept, diffusion and protection of the users.

2. Interception of other ways of telecommunication: the Internet. Because of the complexity of the technology the law requires providers of Internet access must maintain:

    - An updated list of authorized ranges of IP addresses
    - A register of the IP numbers of their subscribers' connections, for a period not less than one year.

3. The protection of workers against the power and control of the employer.

4. The situation of the work e-mail: There is no express regulation about the treatment to the communications nor to the e-mails in particular.

- **Constitution of the Republic of Chile, Art. 19 N.4**: This law established individual constitutional rights to the respect and protection of public and private life.

- **Law 19,628**: On the protection of private life, commonly referred as **"Personal Data Protection Life (PDPL)."**

Workplace Privacy Laws

PDPL applies Law 19,628 'On the protection of private life', commonly referred as 'Personal Data Protection Law' (PDPL)

This law mainly defines and refers to the treatment of personal information in public and private databases.

Last modified: Feb. 17, 2012.
Law 20.575, establishes the limitations on the handling of personal data

Several principles apply to the treatment of personal financial, economic, banking or commercial data:

- Limited disclosures: This type of data shall only be communicated to established commercial entities, and only for the purpose of a credit granting process. It can also be communicated to entities that take part in this evaluation, and only for the aforementioned purpose
- Legitimacy
- Access and opposition
- Information
- Data quality
- Proportionality
- Transparency
- Nondiscrimination

- Use limitation and security in personal data treatment

Discussion

An employer can monitor employees' conduct and communications in the workplace only under certain circumstances and in compliance with employees' constitutional rights concerning intimacy, private life or honor.

Employee monitoring can be carried out only in accordance with information related to work and only as long as the monitoring is notified well-before the actual monitoring takes place.

Chile requires a balance between the employees' rights and the rights of the employer.

Employers can declare certain types of communications as private and not subject to monitoring.

Employee consent is required.

Works Councils may need to be consulted but it is not mandatory – just recommended.

About Teramind

Teramind is a leading, global provider of employee and user activity monitoring, workforce productivity optimization, user behavior analytics, insider threat detection, forensics and data loss prevention solutions. Over 2,000 organizations in finance, retail, manufacturing, energy, technology, healthcare and government verticals across the globe trust Teramind's award-winning platform.

Teramind Inc.
19495 Biscayne Blvd
Suite 606
Aventura, FL 33180

www.teramind.co
hello@teramind.co
+1-212-603-9617