White Paper

Data Loss Prevention and Monitoring in the Workplace: Best Practice Guide for Europe

Who should read this paper

The information in this whitepaper is relevant to Chief Information Officer, Chief Information Security Officer, Audit Practitioner, IT Director, IT Security Practitioner, Risk Officer

Written by Gary E. Clayton
Privacy Compliance Group, Inc.
Dallas, USA
## Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Workplace Monitoring</td>
<td>1</td>
</tr>
<tr>
<td>Best Practices</td>
<td>3</td>
</tr>
<tr>
<td>Appendix A - European Data Protection Laws</td>
<td>7</td>
</tr>
</tbody>
</table>
Introduction

An organisation doesn't need far-flung offices, telecommuting employees or offshore business partners to be at risk for loss of confidential data. It doesn't even need large amounts of credit card data, patient information or valuable source code. All that is required are people and confidential data. And whether accidental or deliberate, data loss can occur whenever confidential information is used or transferred in violation of company policies or regulatory requirements.

The risk of data loss has increased over the last several years as new, revolutionary and ubiquitous communications technologies have been introduced. These powerful mobile devices have made instant access to personal and confidential data crucial to our day-to-day lives. In fact, tablets, smart phones and other devices have blurred the line between our professional and personal lives. As a result, employees use the same devices to electronically connect to fellow employees, customers, prospects as well as our families and friends. Any frequent flyer can confirm this dramatic change. On almost any given airline flight, a stroll down the aisle will reveal almost every passenger using a smart phone, tablet computer or laptop – often all three – and sometimes all at once. This, in turn, creates an environment that is ripe for the misuse, loss and destruction of confidential, personal and proprietary data.

Safeguarding confidential data is a complex challenge for any organization. A growing number of companies are turning to workplace monitoring and data loss prevention (DLP) technology. DLP solutions enable an automated, process-oriented way of identifying and managing confidential data. DLP effectively monitors and protects confidential data.

In EMEA and a growing number of jurisdictions around the world, strict regulatory requirements present what may seem to be a daunting task for companies seeking to implement a DLP strategy. These laws govern workplace monitoring and the collection of personal data. This paper examines the European data protection laws related to workplace monitoring and DLP. This paper will also examine how Symantec's DLP technology can help your company effectively manage compliance with such laws while enhancing the protection of your confidential data.

Workplace Monitoring

Workplace monitoring in Europe is governed by a variety of privacy laws, rules and regulations. In some countries, the laws on telecommunications regulate the monitoring of email and other electronic communications. In other countries, an employer’s rights to monitor employee communications may be governed by collective bargaining agreements, employment contracts or general privacy and data protection legislation. Throughout Europe, however, it is important to understand that privacy is treated as a fundamental human right and, as such, it cannot be bargained away. This view of privacy is well founded in European law, including:

1. Article 8 of the European Convention for the Protection of Human Rights which states: "Everyone has the right to respect for his private and family life, his home and his correspondence."
2. The Treaty Establishing the European Community requires member states to respect the fundamental rights guaranteed by the European Convention.
3. The European Union’s Charter of Fundamental Rights affirms, "[e]veryone has the right to respect for his privacy or her private and family life, home and communications."
Privacy is not, however, an absolute right. Privacy rights must be weighed against other competing interests. This was made clear in Copeland v. United Kingdom where the European Court of Human Rights specifically recognized the rights of an employer to control his business and protect his legitimate interests and weighed them against the employees’ privacy rights.

In the European Union, the Article 29 Working Party has adopted two principal documents related to monitoring in the workplace. In 2001, the Article 29 Working Party adopted Opinion 8/2001 on the processing of personal data in the employment context (“Opinion 8/2001”). In 2002, the Working Party adopted a Working Document on the surveillance of electronic communication in the workplace (“Working Document”). The Working Document’s guiding principle is that an employee does not lose privacy and data protection rights just by becoming an employee. While these documents are not legally binding, they are nevertheless good indicators of how data protection issues are to be determined under the Directive. One reason is that the Article 29 Working Party is comprised of representatives of the data protection officials of the individual member states.

Documents adopted by the Article 29 Working Party are, therefore, very likely to represent the official opinions of the very officials who are charged with enforcing national privacy laws. A second reason is that the political process of adopting a document generally ensures that the opinion of the Working Party has been widely vetted among the members of the European Commission as well as in the capitols of the individual Member States. Even if the Working Party’s opinion does not ultimately become law, it represents the considered opinion of the majority of the data commissioners of the Member States.

Data loss is a complex problem and there is no one single solution that works best in all situations. In addition to choosing the right technology, companies must adopt appropriate policies, provide adequate training and have the support of senior management. The solution must be able to manage security for data in motion, data at rest and data at the end point. It must include the appropriate technology that will reduce your data loss risks and provide the framework for an effective data loss prevention program. Finally, it should also facilitate compliance with privacy and data protection laws and regulations.
Best Practices

The following section identifies a number of best practices that should be adopted as part of a comprehensive data loss prevention program. By following these six best practices, a company will be able to proactively address data loss while minimizing privacy risks involved in workplace monitoring.

#1: Understand general principles for monitoring

#2: Identify the purposes for monitoring

#3: Monitoring must be proportionate

#4: Consultation

#5: Implement technology that fosters compliance

#6: Understand the laws of each country

Best Practice #1 - Understand general principles for monitoring

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.

- Any limitation on the employee’s right to privacy should be proportionate to the likely damage to the employer’s legitimate interests. Or, conversely, monitoring must be proportionate to the risks confronting the employer.

- 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.

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

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

- 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.

- Finally, any surveillance measures should be transparent to workers.
Best Practice #2 - Identify the purposes for monitoring

Identifying the purposes for monitoring is necessary in most European countries and will almost certainly be required in order to negotiate with employees, works councils and data protection authorities. Historically, employers have asserted many business reasons to electronically monitor in the workplace, including:

• To monitor employee productivity in the workplace;
• To protect against unauthorised use, disclosure or transfer of personally identifiable information on employees and customers;
• To maximize productive use of the employer’s computer systems;
• To monitor employee compliance with employer workplace policies related to the use of its computer systems, email systems and Internet access;
• To investigate complaints of employee misconduct, including harassment and discrimination complaints;
• 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 prevent or respond to unauthorized access to employer’s computer systems, including access by computer hackers;
• To protect computer networks from becoming overloaded by large downloadable files;
• To prevent or detect unauthorized utilization of the employer’s computer systems for criminal activities and terrorism;
• To help prepare the employer’s defence to lawsuits or administrative complaints such as those brought by employees related to such claims as discrimination, harassment, discipline or termination of employment; and
• To respond to discovery requests in litigation related to electronic evidence.

A company considering DLP should take the time 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 DLP 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 DLP technology that can assist in identifying specific risks related to data at rest, data in motion and data at the endpoint.

Best Practice #3 - Monitoring must be proportionate

In broad terms, any adverse impact on employees must be justified by the benefits to the employer and others. 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 Privacy Impact Assessment. In other countries, it may be simply required for the employer to consider certain factors such as:

• Identifying clearly the purposes behind the monitoring arrangement and the benefits it is likely to deliver;
• Identifying any likely adverse impact of the monitoring arrangement;
• Considering alternatives to monitoring 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 privacy 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 privacy impact assessment will facilitate successful discussions with national data protection authorities.

**Best Practice #4 - Consultation**

Armed with a privacy impact assessment, a company is prepared to enter into consultations with employees or others. Whether you must engage in such consultations will depend upon a number of factors, including the laws of each country, the size of your company and the existence of any collective bargaining agreements.

This next step cannot be overlooked. It is important for employers to understand the technology they have chosen for monitoring and to be able to explain this to the workers, their unions and other representatives. Remember that in many countries, workers have the right to participate in decisions that impact the conditions of 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 purposes for monitoring, how monitoring will take place, when it will occur and what will be done with the information collected during 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.

**Best Practice #5 - Implement technology that fosters compliance**

When making a choice of your company’s DLP solution, you should keep in mind how the DLP technology addresses the privacy and data protection requirements for workplace monitoring. Symantec Data Loss Prevention was designed to allow customers to effectively monitor the use of confidential information while safeguarding employee privacy. This is accomplished in a number of ways:

- **Compliance with notices and policies** – Symantec DLP enables companies to comply with their privacy notices and policies. This is achieved through policy-based monitoring which focuses on data processing that violates company policies. Symantec DLP only collects transactions that violate policy.

- **Legitimate purposes and proportionality** – Symantec DLP ensures that data collected during monitoring is used only for legitimate purposes. Symantec DLP enables companies to collect only data that violates policies and, then enables companies to ensure that only those individuals with a "need to know" have access to the collected data.

- **Targeted monitoring** – Data must be collected on processed only for legitimate purposes and then collect only such information that is proportionate to the company’s purpose for data monitoring. Symantec accomplishes this in several ways. First, Symantec safeguards an employee’s privacy by treating the individual who sends the email as “need to know”. Second, Symantec collects only data that violates stated policy. And third, Symantec limits access to collected data to individuals who are approved to receive it.

- **Data integrity/accuracy** – Collecting information that does not violate policy or information on the wrong individuals increases a company’s privacy risks. Symantec has greatly reduced these risks by keeping false positives near zero.

- **Security** – Symantec provides security for the data that are collected by providing secure communications of incident data. Additionally, Symantec provides for role-based access to incident information and provides a complete audit trail.

- **Enforcement** – Symantec provides and audit trail for all information gathered during monitoring. Significantly, Symantec maintains the integrity of audits by logging changes to policies and all activities taken in response to an incident.

- **Onward Transfer** – Symantec enables companies to restrict the transfer of personal data thereby reducing risks under the EU Data Protection Directive that may restrict transborder transfers outside of Europe.
• Access – Symantec's audit trail enables companies to easily provide individuals or works councils, unions or other representatives with access to specific information.

**Best Practice #6 - Understand the laws of each country**

Understanding the privacy and data protection laws of the individual European countries is important to the overall management of workplace monitoring. First of all, companies operating or established in a member state are likely to be bound by the laws of that country. Secondly, there are variances among the member states in applying the E.U. Data Protection Directive. Thirdly, in addition to variances, there is a paucity of judicial decisions, regulations or legislative guidance in a number of countries. Finally, understanding these differences is essential to effectively understanding and managing risks.

If workplace monitoring will include interception or 'opening' a worker’s emails or other means of communication, it is important to understand the employer may also have to comply with a country's laws regulating interception of communications. In the United Kingdom and Germany, for example, there are laws that apply to the monitoring of emails. Employers who wish to monitor must be able to comply with the privacy laws and regulations as well as the telecommunication requirements.

Privacy and data protection laws may impose criminal and/or civil sanctions for violations. These sanctions may be imposed against individuals as well as organisations. It is likely that the sanctions will be increased in the next few years. On 25 January 2012, the European Commission published its proposal for a new General Data Protection Regulation. If the regulation goes into effect, significantly harsher penalties of up to 2% of an organisation’s worldwide turnover would be imposed for the most serious privacy violations.7

The next section (Appendix A) provides a detailed overview of the privacy and data protection laws of European countries and how they may regulate the implementation of workplace monitoring or 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 those laws enacted to comply with the E.U. Data Protection Directive;
• **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 key issues related to employee monitoring.

---

7- It is likely to take at least 2 years to finalise the draft regulation and it is planned to enter into force a further 2 years after that finalised text is published in the Official Journal.
Appendix A - European Data Protection Laws

The Member States of the European Union (EU), as well as the members of the European Free Trade Association (EFTA), 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 laws of a number of the EU Member States, the EFTA members and Russia that related to workplace monitoring. In some jurisdictions there may be numerous laws and regulations governing the collection and processing of personal information in the workplace. Accordingly, it is important to understand how these laws may impact a company’s ability to implement data loss prevention technology.

### Austria

**Overview**

Although the Austrian Constitution does not explicitly provide a right to privacy, data protection is a civil right in Austria. Some sections of the data protection law have constitutional status and may only be restricted under the conditions of Article 8 of the European Convention on Human Rights (ECHR). The entire ECHR has constitutional status in Austria and the Constitutional Court often cites Article 8 in cases involving privacy.

**General Privacy Laws**

- The Austrian Personal Data Protection Act (Datenschutzgesetz 2000 or DSG) contains a number of constitutional provisions.

- The Austrian Civil Code provides for damages for violations of privacy. (Civil Code, § 1328a). The Austrian Enforcement Act provides injunctions whenever an individual’s privacy rights are at risk.

**Personal Data Protection Laws and Regulations**


- The Austrian Personal Data Protection Act provides explicit provisions regarding the use of sensitive data in the workplace.

**Workplace Privacy Laws**

- Labour Constitution Act, §§ 91 and 96, provides that the installation of technological facilities that are likely to "touch upon human dignity" may be introduced only with the consent of the works council. Employers must obtain agreement from works council even if employees have given their consent to monitoring. The Labour Constitution Act provides for worker participation in the management of business. Workplaces with more than 5 employees over the age of eighteen are required to establish a works council in which management and employees have equal representation. The consent of the works council is required for "the introduction of automatic systems for the collection, processing and transmission of employee personal data." Employers need not seek the consent of the works council, however, where the processing is authorized or required by law or by a collective bargaining agreement or an individual work contract.

**Discussion**

Austria has no legislation that specifically regulates monitoring in the workplace. There appears to be little disagreement that employers have the right to control and regulate the work process and works councils have often failed to notice the inherent potential for surveillance.
# Belgium

<table>
<thead>
<tr>
<th>Overview</th>
<th>Belgium has strict data protection laws. The general privacy act is the <a href="https://www.legifrance.gouv.fr/eli/loi/1992/12/8/jo">Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data</a>. While Belgium law recognizes the rights of employers to monitor in certain circumstances, their rights are limited and may require consent of the employees and the works council.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Laws</td>
<td>The principle of privacy protection is set forth in Article 22 of the <a href="https">Belgian Constitution</a>: &quot;Everyone has the right to respect for his private and family life, except in the cases and under the conditions stipulated by law.&quot; The right to privacy is directly binding and can be enforced by employees in the labour 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.</td>
</tr>
<tr>
<td>Personal Data Protection Laws and Regulations</td>
<td>Belgium enacted the <a href="https://www.legifrance.gouv.fr/eli/loi/1992/12/8/jo">Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data</a> (BDPA). The BDPA ensures that 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 processing 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.</td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>Workplace monitoring is governed by at least seven different legal documents from different fields of law. For example, Collective Bargaining Agreement No. 81, the <a href="https">Royal Decree of 13 February 2001</a>, the Data Protection Act, Section 124 of the <a href="https://www.legifrance.gouv.fr/eli/loi/1992/12/8/jo">Electronic Communications Act</a> (unauthorized access to electronic communications) and 314bis of the Criminal Code (unauthorized tapping during the transmission). The interplay of these legal documents is explained in a 2011 set of documents issued by the <a href="https">Belgian Privacy Commission</a>. Article 2, §1 of the collective bargaining agreement No. 13 of 13 December 1983 provides that &quot;once an employer has decided to invest in new technology . . . which has important collective consequences for . . . 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 representatives of the employees on the introduction of the new technology.&quot; The principle of secrecy of correspondence is guarded by Article 109d of the law of 21 March 1991 on reform of certain economic public companies which states that &quot;save with consent . . . it is prohibited for anybody, whether carried out by oneself or through a third person, to take cognizance of the existence of data of all kinds that have been transferred by means of telecommunication and that originate from and are destined to other persons&quot;. The Commission for the Protection of Privacy issued Opinion No. 10/2000 of 3 April 2000. The Commission was of the opinion that an employer should not gain access to the content of an e-mail as, in the Commission’s opinion, not proportionate to any interests that the employer may wish to protect. To make matters more complicated, Belgian courts have issued a number of decisions upholding employer rights to monitor if certain conditions were met. In an effort to clarify workplace monitoring, on 13 July 2011, the Belgian <a href="https">Commission for the Protection of Privacy</a> issued a set of documents including a legal report and a number of recommendations and practical guidelines for workplace monitoring.</td>
</tr>
</tbody>
</table>
### Belgium

monitoring. The Commission concludes that there should be a distinction made between the use of a company’s e-mail for private purposes and its use for professional purposes.

The Privacy Commission recommends that companies start by implementing rules and procedures, including the banning the use of e-mail accounts for personal purposes. Companies that do not strictly follow the guidelines must be able to justify that the applicable rules and regulations are still complied with, especially the principles of proportionality, transparency and finality. The Commission also recommends the use of preventive software such as e-mail and web filters rather than more invasive ‘a posteriori’ controls.

If the e-mail system has been set up as recommended by the Commission, the employer can access the e-mail account and the content of the messages that are considered professional in order to ensure the proper functioning of the company.

The Commission strongly opposes relying on consent in the employment context. The Commission still believes it is important for the employer to properly inform employees of any monitoring.

### Discussion

Carefully follow the rules / guidelines and the solutions recently proposed by the Privacy Commission. Prepare policies that clearly establish that the company’s work e-mail system can be used only for business purposes. Allow employees to access their private e-mail accounts at work for private and confidential communications. The Commission’s documents also provide guidance for employers who are not capable of excluding personal and professional use of e-mail.
## Bulgaria

### Overview


### General Privacy Laws

Article 32, para. 1 of the Constitution of the Republic of Bulgaria provides: “The privacy of citizens shall be inviolable. Everyone shall be entitled to protection against any illegal interference in his private or family affairs and against encroachment on his honour, dignity and reputation.”

Other sections of the Constitution protect the confidentiality of correspondence and prohibit the photographing or similar recording of an individual without his knowledge and consent.

Article 1 of the Personal Data Protection Act states that the Act is intended to guarantee the inviolability of individuals and their privacy.


### Personal Data Protection Laws and Regulations

Law on Personal Data Protection

### Workplace Privacy Laws

Bulgaria entered the European Union on 1 January 2007. To date, no laws specifically addressing workplace privacy have been enacted. The Commission for Personal Data Protection has not issued any guidance regarding workplace privacy.

The Labour Constitution Act of 1974, §§ 91 and 96, provides that the installation of technological facilities at work that are likely “to touch upon human dignity” may be introduced only with the consent of the works council.

### Discussion

Until specific guidance is issued or legislation adopted, follow the general principles of 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) when workplace monitoring is in question.

Bulgaria has a number of sector-specific laws that may impact the collection of workplace data, including the Banking and Lending Act, which has provisions requiring bank employees to keep customer information confidential. The Telecommunications Law requires the operators of telecommunications to protect the secrecy of communications and to take all necessary technical and organizational measures to protect communications. It may be argued that such laws impose obligations that may include workplace monitoring to protect the confidential and secret information.
### Cyprus

<table>
<thead>
<tr>
<th>Overview</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>General Privacy Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processing of Personal Data Law of 2001</strong> came into force on 23 November 2001. Pursuant to Section 3(1) of the Law, it applies to the processing of personal data &quot;wholly or partly by automatic means.&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Data Protection Laws and Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing of Personal Data Law of 2001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workplace Privacy Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Processing of Personal Data Law of 2001 applies. The Law, however, does not specifically address monitoring in the workplace.</td>
</tr>
<tr>
<td>The <a href="https://www.coppd.gov.cy/">Office of the Commissioner for Personal Data Protection</a> (COPPD) has issued an Employment Order setting out the rights and obligations related to employee data. Under the Employment Order, employees are entitled to be informed about the sources of their personal data that are being processed, including e-mail monitoring.</td>
</tr>
<tr>
<td>The COPPD’s annual reports indicate that in most years there are few, if any, complaints about workplace monitoring.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring must be proportionate to the risks confronting the employer. Follow the general principles of the Directive and guidelines of the Article 29 Working Party.</td>
</tr>
</tbody>
</table>
# Czech Republic

## Overview
The Czech Republic’s Office for Personal Data Protection (OPDP) has issued its opinion that an employer “cannot under any circumstances monitor the content of correspondence”, including e-mails. According to the OPDP, the "universal principle of mail privacy applies also to communication in the workplace. This communication includes e-mail and files attached to it."

## General Privacy Laws
The 1993 Charter of Fundamental Rights and Freedoms provides for extensive privacy rights for individuals.

## Personal Data Protection Laws and Regulations

## Workplace Privacy Laws
The OPDP issued its Position No. 1/2003 on the monitoring of electronic mail and the protection of employee privacy and personal data. The OPDP applies the laws that protect the privacy of mail and telecommunications to protection e-mails. While recognizing an employer’s need to protect itself and its intellectual property, the OPDP states that e-mail is personal data and fully protected. The OPDP’s opinion states that it must be “emphasized that the employer cannot under any circumstances monitor the content of correspondence – i.e. also electronic correspondence – of his employees or other persons. If the employer wishes to monitor the number of electronic messages delivered or sent, he or she should notify the employees in advance of his intention to do so and include this right explicitly also in the contractual conditions under which the employment takes place.”

The OPDP has allowed monitoring of the titles of employees’ e-mail correspondence. Such monitoring has been broadly discussed but there has been little agreement as to the precise line between an employee’s right to privacy and employer’s authority and economic interests.

## Discussion
Employers should follow the OPDP’s Opinion 1/2003 and treat e-mails as confidential communications that cannot be monitored.

The OPDP’s opinion appears to presume that employers are monitoring e-mail solely to “check whether his employees respect their working hours and how efficiently they use their work time.” The OPDP does not consider whether the employer can monitor to protect personal data or prevent violations of policy although the opinion does seem to leave open the possibility that a number of factors should be considered in "judging whether the employer is justified to use certain methods of monitoring his employees."
## Denmark

### Overview

### General Privacy Laws
The [Danish Constitution of 1953](https://example.com) contains two provisions on privacy: Article 72 provides for secrecy of letters and other papers, and in postal, telegraph and telephone matters.

The [Danish Penal Code, § 263](https://example.com), provides for secrecy of mails and makes it a criminal offense to open or otherwise acquire access to content of a letter or another closed message addressed to another person.

### Personal Data Protection Laws and Regulations
[Act on the Processing of Personal Data](https://example.com) applies to the processing of data undertaken for a data controller established in Denmark provided that the activities take place within an EU Member State or data controllers established in a third country if the data collection took place in Denmark.

### Workplace Privacy Laws
Monitoring and surveillance in the workplace is usually dealt with through collective bargaining agreements. Generally, an employer is allowed to monitor the work done in the workplace but the employer must do so responsibly and not abuse their power.

According to the Annex to the Basic Agreement between the Danish Confederation of Employers and the Danish Confederation of Trade Unions of 24 April 2001, the employer is obliged to inform the employees of any specific monitoring activities that he plans to carry out two weeks in advance of any such monitoring being introduced.

The Danish [Data Protection Authority](https://example.com) has found that a company may examine a "security copy" of an employee and examine the copy if it is necessary for the legitimate interests of the employer and the interests of the employee do not override these interests.

[§ 263 of the Danish Penal Code](https://example.com) applies to e-mails and may be applicable in limited workplace situations.

### Discussion
Although Denmark has been fairly active in legislating privacy protections in specific circumstances, there is little specific guidance on monitoring in the workplace. Monitoring in the workplace is not a widespread practice in Denmark. It is likely that Denmark will follow the guidance of the [Article 29 Working Party](https://example.com).
## Estonia

### Overview

It is not prohibited for an employer to read work-related e-mails of an employee, subject to certain conditions. The Estonian Data Protection Inspectorate has issued [Guidelines for Human Resources Employees: Personal Data in Employment Relationships](6 June 2011)(Guidelines). The Guidelines discuss the measures that should be considered by an employer before monitoring e-mails. Subject to the conditions set forth in the Guidelines, it may also be possible for an employer to read the private e-mails of an employee.

### General Privacy Laws

The [Estonian Constitution](0x0) recognizes the right of privacy, the right to privately exchange information and the right of data protection. Article 43 states that each person has a right for secrecy concerning messages transmitted to him via post, telegraph, telephone or other means generally in use.

### Personal Data Protection Laws and Regulations

[Personal Data Protection Act of 2003](0x0) implements the EU Data Protection Directive.

### Workplace Privacy Laws

On 6 June 2011, the [Estonian Data Protection Inspectorate](0x0) issued the [Guidelines for Human Resources Employees: Personal Data in Employment Relationship](0x0) (the “Guidelines”), which give an overview of the Guidance Notes approved by the Inspectorate on 24 January 2011. The Guidance Notes are available only in Estonian.

Subsection 2(7) of the Guidelines states that "it is not prohibited for an employer to read the work-related e-mails of an employee." The Guidelines, however, advise employers to be careful about reading private messages. The Guidelines discuss only two reasons for reading e-mail in the inboxes of employees: (1) obtaining information that is required for the organization of work; and (2) checking employees. With respect to checking employees, the Guidelines provide that the private messages of an employee may be read if all of the following conditions are met: (1) the obligation the performance of which is checked can be clearly ascertained and it is important; (2) the right to read private messages arises from the employment contract or the employee has given their consent to this; (3) the private message contains no sensitive data; (4) the performance of an obligation cannot be checked in any other manner; (5) it was reasonably possible for the other party to the message to understand that the e-mail address was not the private e-mail address of the employee; and (6) the employee and the other party to the message are both notified of the message being read.

Subsection 41(2) of the Estonian [Employment Contracts Act](12 January 2009) stipulates that an employer must process employee personal data pursuant to the [Personal Data Protection Act](0x0).

### Discussion

Subsection 2.7 of the Estonian [Data Protection Inspectorate](0x0)’s Guidelines contain recommendations that lay out some practical steps that an employer should follow in order to monitor e-mails. These steps include establishing written rules regarding the monitoring of e-mails and the prohibition of using the employer’s e-mail system for personal use. The employer should also inform employees of the measures taken to process data within the organization.
## Finland

<table>
<thead>
<tr>
<th>Overview</th>
<th>Finland’s Constitution guarantees every citizen’s private life and honour and the sanctity of the home. Finland’s <a href="https://www.dataprotection.fi/en">Office of Data Protection</a> has provided significant guidance related to privacy in the workplace.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace Privacy Laws</td>
<td>Finland has the <a href="https://www.finlex.fi/en/laki/2007/en759">Act on the Protection of Privacy in Working Life</a> (759/200), which guarantees limited e-mail privacy for employees. The law also stipulates that the regulation of e-mail privacy is to take place through bargaining and consultation procedures at the workplace level. The law also stipulates that during discussions, the employer must discuss the conditions under which e-mails may be monitored. The Act on the Protection of Privacy in Working Life places the burden on employers to justify the necessity to collect and use information about their employees and potential employees. Chapter 6, § 18 of the Act relates to the &quot;Retrieving and opening electronic mail messages belonging to the employer.&quot; Private e-mail sent from the workplace is given the same protections as postal mail, but employers can prohibit the use of communication facilities for private use. Under Finnish law, the employer must specify the purposes for monitoring and the monitoring methods that will be used. Finnish law also requires the employer to provide notice to all employees regarding the purposes for and means of monitoring. The Office of Data Protection has issued a number of documents providing guidance on workplace privacy. These include the 2008 brochure <a href="https://www.dataprotection.fi/en">Data Protection in Working Life</a> and the 2008 <a href="https://www.olas.fi/en">Study on the Protection of Privacy at Work</a>. Sections 19 and 20 of the brochure Data Protection in Working Life provide detailed guidance on the ‘retrieval’ and ‘opening’ of e-mail belonging to the employer. Employers who plan on monitoring in Finland should follow the guidance provided in the brochure.</td>
</tr>
<tr>
<td>Discussion</td>
<td>Section 19 of the Act on the Protection of Privacy in Working Life gives the employer &quot;the right, assisted by the person vested with the authority of the information system administrator, to find out on the basis of information concerning the message sender, the recipient or title, whether the employee has, in his/her absence, been sent, or has sent or received immediately before the absence, messages belonging to the employer . . . .” The Act, however, places a number of conditions on that right. If the message retrieval does not lead to the opening of the message, the Act requires a</td>
</tr>
<tr>
<td>Finland</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td>report to be prepared and signed by the persons involved stating why the message was retrieved, the time it was retrieved and who performed the retrieval. The report must be submitted to the employee without undue delay, except in limited circumstances. Additionally, the information obtained may not be processed more extensively than necessary for the purpose of retrieving the message, and the persons processing the information may not disclose it to a third party during the employment relationship or after its termination.</td>
<td></td>
</tr>
<tr>
<td>If, on the basis of information on the sender or recipient of an e-mail or the message title, it is apparent that the message belongs to the employee or it contains certain essential information for the employer, then the employer, &quot;with the assistance of the person vested with the authority of information system administrator and in the presence of another person&quot; may open the message. The Act requires the employer to prepare a report, signed by the persons involved, stating which message was opened, why it was opened, the time of opening, the persons performing the opening and to whom the information on the content of the opened message was given. The report must be submitted to the employee without undue delay, except in limited circumstances. As with messages retrieved, but not opened, the information may not be processed more extensively than necessary for the purpose of opening the message. Additionally, the persons processing the information may not disclose to content of the message to any third party.</td>
<td></td>
</tr>
</tbody>
</table>
## France

### Overview

The French [Data Protection Authority (CNIL)](https://www.cnil.fr) is one of the largest data authorities in Europe and actively enforces the French privacy and data protection laws.

The French [Labour Code](https://www.legifrance.gouv.fr) recognizes the employer’s right to monitor the proper performance of work tasks by its employees, provided that such monitoring does not violate the employee’s fundamental rights and freedoms (Art. L 120-2). 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](https://www.legifrance.gouv.fr) provides a right to privacy.

Article 226 of the French [Penal Code](https://www.legifrance.gouv.fr) provides that wilfully infringing someone else’s privacy 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](https://www.legifrance.gouv.fr) relating to the protection of individuals with regard to the processing of personal data.

### Workplace Privacy Laws

In France, the Labour 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. L 120-2). Network monitoring of employees is thus permitted, subject to the protection of the employee’s 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 company systems or otherwise act against the company’s interests 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. (Labour 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 employer 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.
### France

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

<table>
<thead>
<tr>
<th>Overview</th>
<th>Data processing in Germany is generally governed by the <a href="https://en.wikipedia.org/wiki/Federal_Data_Protection_Act_2002">Federal Data Protection Act 2002</a> (&quot;FDPA&quot;) 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. Germany is generally regarded as having the strictest data protection laws in the world. These laws are vigorously enforced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Laws</td>
<td>Article 10 of the <a href="https://en.wikipedia.org/wiki/Basic_Law_%28the_German_Constitution%29">Basic Law (the German Constitution)</a> provides basic privacy protections for letters, posts and communications.</td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>The Works Constitution Act gives works councils co-determination rights over: rules of conduct where the employer permits the use of company e-mail systems 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, then 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 <a href="https://www.gesetze-im-internet.de/estg2004/ESTG_2004_1.pdf">Telecommunications Act of 22 June 2004</a>. 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.</td>
</tr>
<tr>
<td>Discussion</td>
<td>In August 2010, the German Government proposed amendments to German law regarding employee data protection. The amendments, however, have not been enacted nor have they 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.</td>
</tr>
</tbody>
</table>
### Greece

| Overview | The two main data protection laws in Greece are:  
| Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data  
| Protection of personal data and privacy in electronic telecommunications sector and amendment of law 2472/1997  
| The Hellenic Data Protection Authority has issued a decision on monitoring in the workplace: Decision 61/2004 on the Access of the Employer to the Personal Computers of Company Employees. |

| General Privacy Laws | The Hellenic Constitution of 1975, as revised April 1, 2001, contains a set of fundamental rules governing privacy.  
| The Greek Constitution has several provisions on the protection of basic human rights, which includes privacy. |

| Data Protection Authority Decision 115/2001 interprets the norms laid down in laws 2472/1997 and 2774/1999 on data protection for purposes of applying them in the area of employment relationships. |

| Workplace Privacy Laws | Hellenic Data Protection Authority has produced a decision on monitoring in the workplace: Decision 61/2004 on the Access of the Employer to the Personal Computers of Company Employees  
| Data Protection Authority Decision 15/2001 interprets the norms laid down in Law No. 2472/1997 and Law No. 2774/1999 on data protection for the purpose of applying them in the area of employment relationships.  
| Law No. 1767/1998, as amended by Law 2224/1994, grants worker’s councils powers to jointly decide with the employer on certain issues including surveillance. |

| Discussion | Information obtained during monitoring must only be used for specific purposes and must be limited to what is necessary to accomplish the legitimate purposes for monitoring. Employers should carefully craft policies to disclose what monitoring will take place and to ensure that the information is adequately safeguarded. Employees should be given access to their information. The Data Protection Authority specifically endorsed the reasoning and arguments put forth by the Article 29 Working Party in its Working Document on the surveillance of electronic communications in the workplace.  
| Greek law provides for significant monetary fines and imprisonment for violations. |
| **Overview** | On July 26, 2000, the European Commission decided that Hungarian law provided an adequate level of protection of personal data.

On 17 January 2012, the European Commission started legal action against Hungary over new legislation that came into force at the beginning of the year under Hungary’s new constitution. Specifically, the European Commission challenged the independence of the Hungarian data protection authorities.

The Act on Informational Self-Determination and Freedom of Information (the new Data Protection Act) went into effect on 1 January 2012, creates a National Agency for Data Protection to replace the former Data Protection Commissioner’s Office. The EU Commission challenged the termination of the Data Protection Commissioner prior to the end of his term which was due to expire in 2014. |
| --- | --- |

Hungary also has numerous sector-specific laws regulating the protection and privacy of data.

Article VI of the new Constitution provides: "(1) Every person shall have the right to the protection of his or her private and family life, home, relations and good reputation; (2) Every person shall have the right to the protection of his or her personal data, and to access and disseminate data of public interest; (3) The exercise of the right to the protection of personal data and the access to data of public interest shall be supervised by an independent authority."

Article 59 of the Hungarian Constitution reads as follows: "(1) In the Republic of Hungary, everyone is entitled to the protection of his or her reputation and to privacy of the home, of personal effects, particulars, papers, records and data, and to the privacy of personal affairs and secrets." |
| **Personal Data Protection Laws and Regulations** | The new Data Protection Act maintains most of the material provisions of the 1992 law. Section 6(1) of the new Data Protection Act sets out a "balance of interest clause" providing that personal data may be processed if obtaining the consent of the data subject is impossible or if it entails disproportionate expense and data processing is necessary for compliance with legal obligations of the data controller or if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party and the assertion of this interest is proportionate with the interference in the rights for data protection. |
| **Workplace Privacy Laws** | Hungary does not have any specific laws regulating workplace privacy.

The Hungarian Data Protection Office set forth guidance for monitoring at work in its 2001 statement entitled "The employer needs the employee's consent to inspect his electronic correspondence at the e-mail address at the workplace." According to the Data Protection Office, a distinction must be made between "e-mail addresses given to employees for their personal use which may contain a fragment or the entirety of their names, and e-mail addresses for managing the company's affairs that are not tied to individual employees." The employer is entitled to inspect the latter type of e-mails even if the employee has been provided with notice but decides to use it for personal purposes. With respect to the e-mail addresses for employees' personal use, the employer cannot examine, withhold or destroy the e-mails unless he has secured the employee's consent. |
In two opinions issued in 2001 by the Data Commissioner, the conditions for monitoring e-mails. In cases where e-mail is authorized exclusively for work-related purposes, the employer does have the right to monitor, provided that the employees have been warned of the restriction and the possibility of being monitored. If, however, the employer has not issued a policy restricting use to work purposes only, or if the employer has authorized the use of e-mails for personal purposes, then monitoring is not authorized. According to the Commissioner, if an employer logs e-mail or other network activity without meeting these conditions, "he will have controlled data just as illegally as if he tapped the employee's phone lines."

Employers should issue a clear policy stating that the computer equipment, network and communications (including e-mail) are to be used exclusively for business purposes and that they will be monitored. Employers should remind employees of the policy when they log onto their computers. Employers should obtain employee's consent or provide e-mail addresses that do not contain the employee's name.
<table>
<thead>
<tr>
<th>Ireland</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
</tr>
<tr>
<td><strong>General Privacy Laws</strong></td>
</tr>
<tr>
<td><strong>Personal Data Protection Laws and Regulations</strong></td>
</tr>
<tr>
<td><strong>Workplace Privacy Laws</strong></td>
</tr>
<tr>
<td><strong>Discussion</strong></td>
</tr>
</tbody>
</table>
## Italy

### Overview

The Garante per la Protezione dei Dati Personali (Italian Data Protection Authority) aggressively enforces the Italian data protection laws.

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

### 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 implements the EU Data Protection Directive and applies to workplace monitoring.

### 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 Article 8(b) of the Directive on the processing of sensitive data. Section 26(4d) allows the processing of sensitive data without consent if necessary to meet obligations under employment law.

The Code implements parts of the E-Communications Privacy Directive (see Title 10, Part 2 of the 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 March 29, 1983, applies to workplace monitoring but does not prohibit employers’ rights in this area.

Article 4 of the Workers' Statute (Law No. 300/1970) 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 union opinions of workers. The Italian Data Protection Authority has drawn a distinction between workplace monitoring for purposes of controlling employees and "defensive" monitoring.

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

The Italian Supreme Court recently upheld a ruling in favour of an employer who determined that an employee was improperly using customer information via 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 confirmed the decision stating that the aim of Section 4 is to protect the dignity and privacy of employees where an employer’s monitoring would otherwise be invasive. The Supreme Court noted, however, that this implies that employees are engaged only in legitimate activity. The Court confirmed that "defensive monitoring" is not covered by Section 4.
## Italy

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 not intended to ascertain whether employees are carrying out their work correctly. 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 Use of E-mails and the Internet in the Employment Context. Until this has been clarified, companies should, 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 labour 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; and (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: (a) the conditions for using Internet and e-mail at work; (b) the extent to which private use of the Internet and e-mail is accepted in the workplace; (c) the fact that e-mails may be monitored and the specific purposes for monitoring; (d) what kind of information can be stored temporarily and who is authorized to have access to it; (e) the options to be used in the event of an employee’s absence; (f) the security measures in place; (g) the modalities of the monitoring activities; and (h) 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.
<table>
<thead>
<tr>
<th><strong>Latvia</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
</tr>
<tr>
<td><strong>General Privacy Laws</strong></td>
</tr>
<tr>
<td><strong>Personal Data Protection Laws and Regulations</strong></td>
</tr>
<tr>
<td><strong>Workplace Privacy Laws</strong></td>
</tr>
<tr>
<td><strong>Discussion</strong></td>
</tr>
</tbody>
</table>
**Lithuania**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Protection Laws and Regulations</td>
<td>The LLPPD was passed in 1996, and has been amended multiple times. The law is based on standard fair information practices and is fully compliant with the <a href="https://eur-lex.europa.eu/eli/dir/1995/46/24_en">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</a> (EU Data Protection Directive). The <a href="https://eur-lex.europa.eu/eli/dir/1997/272/2005">Law on Electronic Communications</a> protects the confidentiality of electronic communications. Section 63 protects the confidentiality of communications over electronic communications networks and prohibits persons other than the actual users from “listening, tapping, storing or otherwise intercepting information or related traffic data or gaining secret access to such information” except “when legally authorized to do so.” Article 77 lists the situation where such interceptions are authorized. For “undertakings” providing such communications networks, interceptions are authorized “only to the extent that is necessary to ensure economic activities of the said undertakings.”</td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>Lithuania does not have laws specifically addressing monitoring in the workplace. Article 61, Paragraph 1 of the Law on Telecommunications stipulates that the disclosure of information transmitted over electronic communications networks other than the actual users is prohibited unless the users have consented. Article 61, Paragraph 2, also provides, however, that Paragraph 1 shall not affect any legally authorized recording of information when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. Users have to be informed about the recording, its purpose and storage before the recording takes place. Legal scholars in Lithuania have opined that if these procedures are followed, a “high probability emerges that the telephone conversation or electronic mail of an employee can be recorded.”</td>
</tr>
<tr>
<td>Discussion</td>
<td>Lithuania has limited experience dealing with workplace surveillance issues. Companies considering surveillance in Lithuania should adopt a policy specifically stating that surveillance will take place. Notice should be given to the employees and it should provide information on the purpose of monitoring.</td>
</tr>
<tr>
<td><strong>Luxembourg</strong></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td>Luxembourguian law regulates the data processing activities of organizations and individuals who collect and use personal data.</td>
</tr>
<tr>
<td><strong>General Privacy Laws</strong></td>
<td>Article 29 of the Constitution protects the secrecy of correspondence.</td>
</tr>
<tr>
<td><strong>Personal Data Protection Laws and Regulations</strong></td>
<td>Law of 2 August 2002 (French only) on the Protection of Persons with regard to the Processing of Personal Data 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 2002 Act created a new data protection authority, the Commission nationale pour la protection des données, also known as the CNPD. The CNPD became operative on December 12, 2002. It controls the processing of personal data in Luxembourg and ensures compliance with the data protection regulations.</td>
</tr>
<tr>
<td><strong>Workplace Privacy Laws</strong></td>
<td>Workplace monitoring is governed by law. The Law of May 6, 1974, establishing joint works committees in private sector provides employees with co-determination rights on the introduction and application of technical equipment designed to monitor employees’ behaviour and performance at their work stations. An authorization from the CNPD is required before using technical means for monitoring.</td>
</tr>
<tr>
<td><strong>Discussion</strong></td>
<td>Luxembourg has limited experience dealing with workplace surveillance issues. Companies considering surveillance in Luxembourg should adopt a policy specifically stating that surveillance will take place. Notice should be given to the employees and it should provide information on the purpose for monitoring. Luxembourg also has numerous laws on financial secrecy. In December 2001, the Commission of Surveillance of the Financial Sector (Commission de Surveillance du Secteur Financier) released practical and technical guidelines to financial services companies that intend to promote the protection of customers’ privacy and the confidentiality of their financial information when launching new online financial services.</td>
</tr>
<tr>
<td><strong>Malta</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td>Malta enacted a comprehensive data protection act in 2001. The Act, however, does not specifically give guidelines about privacy issues at work although most of the Act's sections apply to the workplace.</td>
</tr>
</tbody>
</table>

Article 32 of Malta’s Constitution provides for protection of an individual’s “private life.”

Article 41 of the Constitution provides for protection of “correspondence.” |

Pursuant to Article 36, the Information and Data Protection Commissioner is charged with enforcing data protection in Malta.

Article 29 et seq. mandates that data controllers must register data processing with the Commissioner prior to commencement of the processing. Section 29(3) lists the information that must be provided to the Commissioner before processing can take place. |
| **Workplace Privacy Laws** | The Data Protection Act is the main regulatory framework in Malta regarding privacy in the workplace. The Act provides nine principles of “good information handling” to guarantee the protection of personal information. Under these principles, employers are obliged to inform individuals of the reasons for collecting personal information about them. Additionally, individuals are to be assured that the data collected will not be used for any reason apart from that specified by the data controller.

The Act, however, does not specifically give guidelines about privacy issues at work although most of the Act's sections apply to the workplace; (2) to question the employer about the kind of data kept in their employment files; (3) to know whether work e-mails are monitored; and (4) to be made aware of the purpose for which data about them are collected.

To date, collective bargaining in Malta does not cover the issue of workers' privacy in the workplace although unions may negotiate directly with a company's management if privacy issues arise. It appears that the largest unions in Malta have never brought forward to the Industrial Tribunal any disputes about the use of monitoring in the workplace. |
| **Discussion** | The Commissioner’s office has previously promised to issue guidance on workplace monitoring but none has been issued to date. Until additional guidance is provided, companies should follow the general principles of the Directive and the guidance provided by the Article 29 Working Party. |
### Netherlands

#### Overview

Article 10 of the [Constitution of the Netherlands](#) guarantees the right of privacy.

The Netherlands has been active in promoting personal data protection. The legal framework for privacy consists of general constitutional protection, a general data protection law, and employment law.

#### General Privacy Laws

Article 10 of the Dutch Constitution states that all citizens are entitled to respect of their personal privacy.

Article 13 of the Constitution guarantees privacy of correspondence, telephone and telegraph communication.


#### Personal Data Protection Laws and Regulations

The [Personal Data Protection Act](#) applies generally to all processing of personal data. Article 27 of the Act requires data controllers to file a notification prior to commencement of automatic data processing. Article 28 lists the information that must be provided in the notification.

#### Workplace Privacy Laws

Article 7:611 of the [Dutch Civil Code](#) requires employers and employees to act in good faith. This concept of ‘good employership’ gives effect to the right of privacy for employees. The Personal Data Protection Act also applies to employer/employee relationships. The Works Council Act (1979) is applicable to the processing of personal data by employers. An employer who intends to implement, alter, or withdraw rules for the processing of employee data needs the works’ council’s consent.

The Data Protection Authority has taken a practical approach to privacy in the workplace. “During working hours, people do not have the same freedoms they have outside these hours. An employee is, however, entitled to privacy at the workplace and protection of his or her personal data that are processed within the scope of the employment relationship.

“Checking on e-mail is not prohibited.” An employer is entitled to set conditions for the use of e-mails and must set down the reasons why he believes control is necessary.

The Dutch Works Councils Act requires every Dutch enterprise consisting of 50 or more employees to elect a works council from the employee workforce. The works council must be consulted on certain management decisions affecting the employees and the enterprise, which may not be implemented without their formal approval. The Works Council Act requires that any decision concerning the recording, processing, or protection of employee personal data must be ratified by the works council.

In 2000, the [Dutch Data Protection Authority](#) published a study entitled Working Well in Networks, which covers monitoring, the use of the Internet and e-mail in the workplace. As a result, the Dutch Data Protection Authority formulated rules of thumb for employers who check their employees’ use of the Internet and e-mail. The Dutch Data Protection Authority also developed a legal framework for the use of e-mail and the Internet in the workplace. The
Netherlands

Following 17 “rules of thumb” were set out by the Data Protection Authority: (1) Treat businesses online in the same manner as offline; (2) Set up clear rules with agreement of the works council; (3) Publish the rules in a way that is accessible for the employee; (4) Determine to what extent private use of the facilities is permitted and which software may be used for this; (5) As far as possible, use software to prevent prohibited uses; (6) Make reports and user statistics anonymous; (7) Take into consideration the system back-ups; (8) Guarantee the integrity of the system manager; (9) Discuss doubtful behaviour with the person concerned as soon as possible; (10) Grant inspection of the data; (11) Evaluate the rules periodically; (12) Make sure business and private mail are separated. If not possible, avoid private mail as much as possible; and (13) Limit controls to the objective formulated. Provide for control mechanisms geared to this; (14) Carry out the control on observance as little as possible (tailored work); (15) Limit the logging of network use to the data traffic (e-mail) or the data that are necessary for the aim; (16) Save the logged data no longer than necessary; and (17) Avoid privileged information from members of the works council and company doctors in electronic messages.

Discussion

The Dutch Data Protection Authority recognizes that employers have the right to set the terms and conditions for the use of the network, e-mail and the Internet. Employers should establish a written policy, setting forth the terms and conditions for the use of the network, e-mail and communications and giving notice to employees that monitoring will take place. Employers should notify employees of the reasons for workplace monitoring. Employers should weigh the various forms of monitoring and then choose the “least drastic means.” Employers should consider how to comply with the 17 rules of thumb listed above. The employer should document its assessment of the 17 rules of thumb and why (or why not) they apply to the facts and circumstances of their workplace. Employers should consider conducting and/or following an assessment based upon the Privacy Audit Framework under the Dutch Data Protection Act issued in 2001.
<table>
<thead>
<tr>
<th>Overview</th>
<th>Norway enacted its <a href="https://www.privacyresources.org">Personal Data Protection Act</a> in 2000. Although Norway is not a Member State of the European Union, the Personal Data Protection Act was intended to bring Norway into compliance with the <a href="https://eur-lex.europa.eu">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</a> (EU Data Protection Directive). There is limited guidance on the use of surveillance in the workplace due to the limited use of workplace monitoring in Norway.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Laws</td>
<td>The Norwegian Constitution does not explicitly provide the right to privacy. Norwegian courts, however, have established a fundamental legal principle of “protection of personal integrity.” The principle is similar to privacy principles in other European nations.</td>
</tr>
<tr>
<td>Personal Data Protection Laws and Regulations</td>
<td><a href="https://www.privacyresources.org">Personal Data Protection Act</a> is supplemented by <a href="https://www.privacyresources.org">Personal Data Regulations</a> (the ‘Regulations’).</td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>A new Chapter 9 to the Regulations deals with monitoring of employee e-mail and came into effect on 1 March 2009. Under Chapter 9, an employer may &quot;only explore, open or read e-mail in an employee’s e-mail box (a) when necessary to maintain daily operations or other justified interest of the business; (b) in case of justified suspicion that the employee’s use of e-mail constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal. Chapter 9, § 3 provides the procedures for examination, which include: notifying the employee wherever possible and giving the employee an opportunity to speak before the examination is made. The employer, wherever possible, shall provide the employee with the opportunity to be present during the examination, and shall have the right to the assistance of an elected delegate or other representative. If the examination is made with no prior warning, the employee shall be entitled to receive written notification of the examination as soon as it is done.</td>
</tr>
<tr>
<td>Discussion</td>
<td>Employers should establish a written policy regarding workplace monitoring. The policy and/or other notice should provide information on how the monitoring will take place, the employees’ rights, etc. Where possible, the monitoring should leave an audit trail, quarantine e-mail messages that violate policy and provide notice to the employee and opportunity to be present when the e-mail is reviewed.</td>
</tr>
</tbody>
</table>
Poland

<table>
<thead>
<tr>
<th>Overview</th>
<th>Polish law does not provide specific rules for monitoring in the workplace and Polish courts have not dealt with the issue in detail. Also, there is no specific guidance from the Inspector General for the Protection of Personal Data (GIODO). GIODO has not provided guidance on the permissible scope of workplace monitoring; therefore, employers are left to the general labour and data protection rules. The Ministry of Labour and Social Policy has provided guidance, which is discussed below.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Laws</td>
<td><strong>Protection of Personal Data Act</strong> and several other laws address privacy and data protection in Poland. The Protection of Personal Data Act fulfils Poland’s obligations as an EU Member State to implement 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).</td>
</tr>
<tr>
<td>Personal Data Protection Laws and Regulations</td>
<td>The <strong>Protection of Personal Data Act</strong>’s principles govern the processing of personal data within Poland.</td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>The Polish <strong>Ministry of Labour and Social Policy</strong> has stated that the current labour law provides sufficient grounds to assume that employee monitoring is legitimate. E-mail monitoring is permitted within the following general principles: (1) the employer is entitled to safeguard their interests and to verify the work of employees; (2) the Labour Code requires an employer to respect the dignity and other personal interests of employees. Additionally, the Minister of Labour and Social Policy issued a regulation that applies to all forms of work where computers are used and prohibits using quality control mechanisms on employee work product if these are implemented without the employees’ knowledge. This means that e-mail monitoring is legitimate if notice is provided. However, employers must not monitor private communications of employees. Employee consent to such monitoring is not effective since Polish courts and GIODO contest consent in the context of employment.</td>
</tr>
<tr>
<td>Discussion</td>
<td>Pending specific guidance from GIODO or other Polish officials, employers should provide employees with a blanket notice. Notice can be included in the employment contract and in the internal work regulations communicated to all employees. Employers should also consider using a notice on the e-mail system or a pop-up warning window on an employee’s screen when they log in. Employers should: (1) Clearly set out rules on the use of work computers and software for private purposes; (2) Clearly explain whether private e-mail is permitted and the conditions and limitations of such use; (3) Clearly explain the consequences of unauthorized private use of the network system. Employers should consider providing employees with two e-mail accounts (one for professional and one for personal use); (4) Provide notice that professional communications will be monitored; (5) Explain the purpose of monitoring, how employee data will be collected and to whom it will be disclosed; (6) Explain whether monitoring applies to all employees within the company or just to selected sections; and (7) Seek employee consent or GIODO authorization if data obtained through monitoring is to be</td>
</tr>
<tr>
<td>Poland</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>transferred to a parent company or an affiliated entity located outside of the EEA in a country that is not considered to provide adequate protection.</td>
<td></td>
</tr>
<tr>
<td><strong>Portugal</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td>Companies considering monitoring in Portugal should carefully read and follow the Data Protection Authority’s recommendations and consult with employees prior to implementing workplace monitoring.</td>
</tr>
<tr>
<td><strong>General Privacy Laws</strong></td>
<td>The Portuguese Constitution recognizes rights to personal identity, privacy of correspondence and other private communication and data protection.</td>
</tr>
<tr>
<td><strong>Workplace Privacy Laws</strong></td>
<td>The Portuguese Data Protection Office has issued Recommendations of the Portuguese DPA Regarding the Monitoring of Employees at the Workplace. The DPA states that it will evaluate all aspects of the data processing and weigh the interests of the employer and the employee. Before starting monitoring, the employer must inform the employees about the details of the monitoring, its purposes, the control methods adopted, how the data will be processed and stored and the consequences of misuse of the communications systems made available to the employees. The Principle of Proportionality applies. The employer must set up “clear and precise rules on the use of the e-mail and Internet access for private purposes, which shall be based on the principles of adequacy, proportionality, mutual collaboration and reciprocal trust. The rules must be submitted to the employees and their representatives for their opinion. Communications that are intercepted/opened may not be disclosed to third parties. The “employer shall not undertake a permanent and systematic monitoring of the employees’ e-mail. The control shall be punctual and towards the areas or activities that present a greater “risk” for the business.” “Monitoring for the prevention or detection of commercial secrets disclosure or detection of commercial secrets disclosure shall be directed exclusively for the employees with access to those secrets and only where there are grounded suspicions.” Access to e-mail communications shall be limited to watching the addresses of the recipients, the subject, date and hour. If the employee designates an e-mail message as confidential and objects to its reading by the employer, then the employer must refrain from reading the contents of the e-mail.</td>
</tr>
<tr>
<td><strong>Discussion</strong></td>
<td>Employers must adopt a clear policy on the use of company on the use of company communications equipment and disclose to the employee that monitoring will take place. Employers must provide information to the employees on the</td>
</tr>
</tbody>
</table>
Portugal

monitoring and consult with the employees or their representatives prior to commencing monitoring. Employers should conduct an assessment to determine specific areas of risk and to verify that monitoring is appropriate to mitigate the risks that have been identified. Monitoring should target violations of the policy and, where possible, should be designed to ensure that e-mails or other communications that are marked “private” are not read. Employers should consider technology that blocks the e-mail before it departs the employer’s network and/or ensure that the employees receive immediate notice. An audit trail should be kept.
### Romania

<table>
<thead>
<tr>
<th>Overview</th>
<th>Other than general privacy rights in the Romanian Constitution, the country has little regulation of workplace privacy or guidelines for workplace monitoring.</th>
</tr>
</thead>
</table>
| General Privacy Laws | Article 26 of the [Romanian Constitution](#) provides the principle according to which public authorities must respect and protection privacy and private and family life.  

Article 195 of the Romanian [Criminal Code](#) (regarding violation of correspondence secrecy) makes it a crime to open, without being entitled, correspondence addressed to another person, or to intercept a conversation via phone, telegraph, or other means of distance transmission, as well as disclosure of correspondence content (even if such correspondence was sent open or was accidentally opened). The terms used by the law ("opening of mail and correspondence") also includes accessing e-mail content by whatever means. |
<p>| Personal Data Protection Laws and Regulations | <a href="#">Law no. 506/2004 on the protection of privacy in the electronic communications sector</a> provides for the confidentiality of communications on “public electronic communications networks and publicly available electronic communications services.” Article 4 prohibits the listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data are prohibited on public networks. No similar law exists for private or corporate networks. |
| Workplace Privacy Laws | Romania has not enacted legislation specifically addressing workplace privacy. There has been little regulatory guidance or enforcement of workplace privacy. |
| Discussion | Since there is little or no guidance or legislation on monitoring in the workplace, follow the general principles set forth in the <a href="#">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</a> (EU Data Protection Directive). Also, consider that in Romania, employees are generally bound to their employers by broad agreements outlining rights, duties and rules of conduct related to their job. Companies should, therefore, consider implementing a monitoring policy that is detailed and unambiguous. Internal rules/regulations should be implemented and these should follow the requirements of Romanian employment law. |</p>
<table>
<thead>
<tr>
<th>Overview</th>
<th>Privacy and data protection laws and regulations are relatively new issues in Russia. Russia’s legislation is modelled on the EU Data Protection Directive but does not meet all of the Directive’s requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Laws</td>
<td><strong>Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ On Personal Data</strong> was amended and made public on 27 July 2011, but made effective retroactively to 1 July 2011. The amendments focus primarily on data transfers. This law is intended to be an omnibus law and applies to all kinds of personal data in the Russian Federation. The Criminal Code imposes criminal liability for the invasion of privacy, which includes violating the secrecy of communications and unauthorized access to legally protected computer information.</td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>The Russian Labour Code does not specifically address monitoring by an employer.</td>
</tr>
<tr>
<td>Discussion</td>
<td>Under the Federal Law, data operators are required to notify the Federal Service on Control of Communications before personal data are processed. This is not required in certain cases, including: (1) In some instances concerning employment relations with an individual, where the data are strictly necessary for the purposes of employment; and (2) Contractual relations with an individual.</td>
</tr>
</tbody>
</table>
## Slovakia

<table>
<thead>
<tr>
<th>Overview</th>
<th>Slovakian law provides little guidance on employee privacy rights or workplace monitoring.</th>
</tr>
</thead>
</table>
| General Privacy Laws | The [Slovakian Constitution](#) provides a number of privacy rights.  
Article 16 provides: “The right of every individual to integrity and privacy shall be guaranteed. This right may be limited only in cases specifically provided by law.”  
Article 19 provides that everyone has the right to protection against unwarranted interference in his private and family life and to protection against the unwarranted collection, publication, or other illicit use of his personal data.  
Article 22 provides: (1) Secrecy of letters, other communications and written messages delivered by post and of personal data shall be guaranteed. (2) No one shall violate the secrecy of letters, neither the secrecy of other communications and written messages kept private or delivered by post or otherwise; save in cases laid down by a law. The same applies to communications delivered over telephone, telegraph or other similar equipment. The privacy of correspondence and secrecy of mailed messages and other written documents and the protection of personal data are guaranteed.” |
| Personal Data Protection Laws and Regulations | [Protection of Personal Data Protection Act](#) |
| Workplace Privacy Laws | Slovakia has no legislation directed to regulating workplace monitoring. |
For additional information, consult with the website of the [Office of Personal Data Protection](#). |
### Slovenia

#### Overview
In many areas, Slovenia’s [Personal Data Protection Act](https://example.com) exceeds the requirements of 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](https://example.com) (EU Data Protection Directive). In the area of workplace monitoring, however, the Slovenian Information Commissioner’s [2010 Annual Report](https://example.com) specifically notes that Slovenian law regulating workplace communications is legally inadequate. In 2009, the [Information Commissioner](https://example.com) prepared draft legislation to address the privacy-related issues of workplace communications but the government has not implemented the proposed act.

#### General Privacy Laws

<table>
<thead>
<tr>
<th>Topic</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Protection Act</td>
<td>Slovenia has ratified the <a href="https://example.com">Convention for the Protection of Individuals with Regard to the Processing of Personal Data</a>.</td>
</tr>
</tbody>
</table>

#### Personal Data Protection Laws and Regulations

The Slovenian Information Commissioner has provided conflicting guidance on workplace monitoring. The Information Commissioner’s [2010 Annual Report](https://example.com) notes that employers “have the right to control the equipment they own and to monitor to a certain extent that such is used in accordance with the purpose for which it was given to employees . . ..” This statement should be considered in light of the Information Commissioner’s previous discussions on workplace privacy.

The Information Commissioner’s website has an [FAQ](https://example.com) section. FAQ 4 asks: “Can my superior examine my e-mail?” The Information Commissioner provides the following answer: “No. The content of your e-mails is protected directly by Article 37 of The Constitution of the Republic of Slovenia (Protection of Privacy of Correspondence and Other Means of Communication), however the Commissioner is not competent to make decisions in this specific area (the applicant has the option of action for compensation, or initiation of criminal law procedure). Additionally, theorists have developed a premise, based on decisions of European Court of Human Rights, which states that even traffic data (to whom you have sent the mail and who sent it to you) is protected in this context. Traffic data forms a personal data filing system, and the employer requires your consent if he/she wishes to access it.”

On 17 July 2008, the Information Commissioner’s office issued its [Opinion 0612-145/2008/9 on Communication privacy and e-mails regarding competencies of Competition Protection Office](https://example.com) (Opinion). Although the Opinion primarily addresses inappropriate investigative measures taken by the Ministry of Economy Competition Protection Office, it does address the privacy of e-mail communications. The Opinion states: “Copying, opening, examining and the use of electronic mail of a person means encroaching into the privacy of individuals, i.e., the right to privacy of letters and other means of communication. This is the so-called communication privacy which is guaranteed by Art. 37 of the Constitution" of Slovenia. . . The scope of protection of communication privacy from Art. 37 of the Constitution . . . is based on the need to protect the confidentiality of relations of an individual when communicating, and not on the type,
### Slovenia

status, or ownership of communication means. . . Art. 37 protects the confidentiality of letters and other means for which an individual justifiably expects privacy; the confidentiality of letters and other means must not be encroached if that would mean violation of human privacy.”

The Information Commissioner’s Opinion continues: “At this point double protection of electronic mail needs to be mentioned. Double protection means that data are protected twice: by provisions under Art. 37, and Art. 38 of the Constitution of [Slovenia], the former protecting the content, and the latter protecting the so-called transport history (e-mail address, who communicated with whom and when).”

<table>
<thead>
<tr>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Until specific legislation or more consistent guidance is provided, proceed with caution before engaging in workplace monitoring of e-mail and other means of communication. Assess the purposes of monitoring and communicate the purposes and means with employees. Obtain written consent or acknowledgement from employees before monitoring takes place.</td>
</tr>
</tbody>
</table>
## Spain

### Overview

The Spanish [Data Protection Act](Organic Law 15/1999) is an omnibus act. Spain's [Data Protection Commissioner](https://www.agpd.es) is active in enforcing privacy rights. Spain has a number of laws protection personal privacy.

### General Privacy Laws

Article 8 of the [Spanish Constitution](https://www.constitution.org) 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.

### Personal Data Protection Laws and Regulations

- [Royal Decree 1720/2007](https://www.gob.es) of 21 December, which approves the regulation implementing [Organic Law 15/1999](https://www.constitution.org), of 13 December, on the protection of personal data.
- [Royal Decree 994/1999](https://www.gob.es), of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data.
- [Article 32/2003](https://www.gob.es) of 3 November (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 Labour Act give employers the right to direct the labour activity and to monitor or supervise employees' work-related obligation – but these rights must not impinge the dignity of the workers.

Data Protection Authority has rendered decision that the Spanish Privacy Act allows monitoring of e-mails if the workers have been previously notified of the surveillance.

### Discussion

The [Guide: Data Protection in Labour Relations](https://www.gob.es) is available in English on the website of the Spanish Agency for the Protection of Data. The Spanish Agency notes that it and the courts have previously “indicated different scenarios in which [surveillance] is acceptable and the conditions in which it can be carried out.” (Page 24). Employee consent is not required since the employer is processing personal data under Section 6.2 of the LOPD. Employers must comply with the principle of proportionality. Under Article 20.3 of the LOPD, the purpose must be to verify the compliance by the worker with his labour obligations and duties.

The Data Protection Agency makes it clear that adequate notice should be given. The notice must describe “in detail the extent to which workers may use the company’s communications systems for their private or personal use. It is also recommended that this includes the purpose of monitoring, information on the monitoring measures adopted, and when it might have an impact on the resources normally used by the worker.” If the measures have an influence on the
Spain

whole of the business, “it is advisable to also provide information to the workers’ representatives on the policies adopted in this matter.”

Employers should consider: (1) establishing a policy and specifically set forth the right to monitor; (2) provide notice to employees before monitoring takes place. The notice should provide a clear description and explanation of why it is necessary to monitor; (3) employers should state that e-mails are the property of the company; (4) employers should focus their monitoring on violations of policy; (5) provide notice to workers’ representatives; and, (6) keep an audit trail and consider having employee representatives or third parties participate / observe the process to ensure it is conducted fairly.
### Sweden

<table>
<thead>
<tr>
<th>Overview</th>
<th>Complies with the EU Data Protection Directive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Privacy Laws</td>
<td>The Swedish <a href="#">Personal Data Act</a> (PDA) was enacted in 1998 to bring Swedish law into conformity with the requirements of the <a href="#">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</a> (&quot;EU Data Protection Directive&quot;). The PDA essentially incorporates the EU Data Protection Directive into Swedish law. The <a href="#">Constitution of Sweden</a> provides for the privacy of correspondence and the confidentiality of communications.</td>
</tr>
<tr>
<td>Personal Data Protection Laws and Regulations</td>
<td><img src="#" alt="Personal Data Act" /> <img src="#" alt="Personal Data Ordinance" /></td>
</tr>
<tr>
<td>Workplace Privacy Laws</td>
<td>Monitoring of e-mails is regulated by the <a href="#">Swedish Penal Code</a> and the Data Protection Act.</td>
</tr>
<tr>
<td>Discussion</td>
<td>The Swedish <a href="#">Data Inspection Board</a> has published a <a href="#">Checklist</a> (in English) that should be followed. Employers should make clear the extent of employees’ rights to use the Internet and e-mail for private purposes. If an employer wants to restrict the employees’ use of the Internet and e-mail, this should be made clear by the guidelines and information provided. It should be clear how the check is carried out. If the employer may go through the content of an employee’s private e-mail messages, this must be made clear by regulations and information provided. The employer must make clear what kinds of measures will be taken if employees violate the policies. Employers should make it clear how long it will keep the data that is the basis of the checks of the employees’ use of the Internet and e-mail. The Data Commissioner’s Office has also published a <a href="#">Summary</a> (in English) of workplace monitoring practices in Sweden.</td>
</tr>
</tbody>
</table>
### Switzerland

#### Overview

Although not a Member State of the European Union, Switzerland is a member in the European Free Trade Association and has adopted data protection laws similar to those of the European Union.

Pursuant to Opinion 5/99 of the Article 29 Working Party, Switzerland has been held to provide “adequate protection” under the EU Data Protection Directive.

Switzerland, like the European Union, has entered into an agreement with the United States related to data protection. The [U.S. / Swiss Safe Harbour Framework](https://www.privacyshield.gov/) provides a convenient method for meeting Switzerland’s adequate protection requirements for personal data.

#### General Privacy Laws

- [Ordinance of 14 June 1993 to the Federal Act on Data Protection](https://www.admin.ch/ch/d/1993/1461.html)

#### Personal Data Protection Laws and Regulations


#### Workplace Privacy Laws

Section 328 of the Code of Obligations establishes the general conditions for workplace monitoring.

The Federal Data Protection and Information Commissioner’s website contains guidance on [Spyware in the workplace](https://www.eda.admin.ch/eda/en/home/data-protection/monitoring.html) that states: “Employers are perfectly entitled to verify the output of their employees as well as the use of the IT equipment that is put at their disposal (PC, e-mail, internet, etc.). However, they have no right to monitor their every move, and must respect certain rules. For example, they must inform employees clearly as to how IT equipment is meant to be used (rules of use). Furthermore, they must explain clearly that compliance will be checked and that any infringement may be sanctioned. They must also spell out what exactly is likely to be checked and how this will be done.”

The Federal Data Protection and Information Commissioner has issued a number of statements that appear to make the monitoring of e-mail difficult, if not illegal. Unfortunately, the guidance documents issued by the Commissioner do not specifically state that monitoring in the workplace is illegal. Instead, the Commissioner has identified a number of measures that would be considered illegal and thus should be avoided by employers.

Employers should have in place clear policies that set forth the proper uses of networks, e-mails, Internet and other electronic communications media. If monitoring is to take place, the employer should set forth the specific basis for monitoring, explain how and when monitoring will take place, and provide information to employees sufficient to enable to employee to understand his or her rights of access, etc. Where feasible, the employer should obtain an employee’s specific consent to monitoring. Monitoring should be tailored to target specific violations of policy – and where possible, immediate notice should be provided to the employee for suspected violations.
<table>
<thead>
<tr>
<th>Switzerland</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to avoid privacy problems, employers should consider setting up employee e—mail accounts in such a manner as to designate that are for business purposes and to avoid the use of an employee’s name. The Swiss Data Protection Commissioner provides the following examples: <a href="mailto:hans.meier@companyname.ch">hans.meier@companyname.ch</a> or <a href="mailto:hans.meier@sales.companyname.ch">hans.meier@sales.companyname.ch</a> (as possibly indicating personal use is permissible), on the one hand, and <a href="mailto:info@companyname.ch">info@companyname.ch</a>, <a href="mailto:sales@companyname.ch">sales@companyname.ch</a>, or <a href="mailto:salesmanager@companyname.ch">salesmanager@companyname.ch</a> (as indicating business purposes only and thus avoiding privacy issues). The Commissioner has made the following statement: “Opening e-mails where there is uncertainty over their nature is not permitted, irrespective of whether private e-mails are allowed within a company or not.” In such circumstances, an employer must consult with the employee to determine the nature of the communication. The Commissioner specifically states: “The name address should be used for purely personal business related correspondence (e.g., personal matters or personal messages.”)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Swiss Data Protection and Information Commissioner has issued the following guidance on spy programs: &quot;It amounts to a high-performance system for monitoring the conduct of employees in workplace and therefore constitutes a violation of the prohibition of the surveillance of other persons' activities as well as the principle of good faith. The recording, monitoring, analysis, storage and processing of information and activities of any nature on the computer without the consent of the person affected is, in our opinion, a breach of secrecy and privacy through the use of a recording device in terms of the Penal Code. Equipped with surveillance and recording functions, the PC becomes a recording device. The private domain in the workplace is protected both under employment law and by the constitutional principle of the secrecy of telecommunications (cf. BGE 126 I 50). Due to the multitude of functions and programming possibilities that surveillance programs provide, the invasion of the privacy of an employee can in certain circumstances be even more far-reaching than in the case of the use of a video camera. The Swiss Federal Supreme Court has yet to issue any judgements (sic) on the use of electronic surveillance software.”</td>
</tr>
<tr>
<td><strong>United Kingdom</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Overview</strong></td>
</tr>
<tr>
<td><strong>Personal Data Protection Laws and Regulations</strong></td>
</tr>
<tr>
<td><strong>Workplace Privacy Laws</strong></td>
</tr>
<tr>
<td><strong>Discussion</strong></td>
</tr>
</tbody>
</table>
About Symantec
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website http://www.symantec.com

UK Headquarters
Symantec (UK) Limited
350 Brook Drive
Green Park
Reading
United Kingdom
RG2 6UH
Tel: +44 (0)870 243 1080
Fax: +44 (0) 870 243 1081

Symantec helps organizations secure and manage their information-driven world with IT Compliance, discovery and retention management, data loss prevention, and messaging security solutions.

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
The information provided in this document is for informational purposes only and is not intended to and does not constitute legal advice or a solicitation for the formation of an attorney-client relationship. The information provided may not apply to your particular facts and circumstances. Information provided may not reflect the most recent developments in the law and may not be applicable to your particular jurisdiction. You should, therefore, seek legal counsel prior to relying on any information provided.
9/2012 21263455