PRIVACY
Compliance Group

Managing Workplace Monitoring in Europe and the EU

Part II of a Series on Protecting Confidential Information and Workplace Privacy

Report Prepared By:
Gary E. Clayton
Privacy Compliance Group, Inc.
8150 North Central Expressway
Suite 1900
Dallas, Texas 75206
Dallas, Texas 75206
Telephone: 214-365-1665
www.privacycg.com
gclayton@privacycg.com

PRIVACY COMPLIANCE GROUP, INC.

MANAGING WORKPLACE MONITORING IN EUROPE AND THE EU

Notice

PCG is a privacy and data protection consulting and technology company. Although PCG may employee licensed attorneys and accountants, the information in this paper is not intended to be legal or accounting advice. If your organization requires such advice, you should consult your own professional adviser.

If you have questions or would like additional information on the matters discussed in this paper, please contact Gary E. Clayton at gclayton@privacycg.com or via telephone at (214) 365-1665.

Privacy Compliance Group, Inc.
January 14, 2008

Table of Contents

Workplace Monitoring in Europe and the EU

Introduction

> *[T]he Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8 [of the Convention for the Protection of Human Rights and Fundamental Freedoms].*
>
> *Copland v. United Kingdom*
> *European Court of Human Rights*[1]

The United States and the European Union (EU)[2] have taken significantly different approaches to protecting the privacy of their citizens. To date, the US has legislated privacy laws by industry sector. The US has eschewed comprehensive legislation and instead relies on a combination of legislation, regulation, and self-regulation. The EU, on the other hand, has adopted comprehensive principles that regulate all aspects of processing personal data. The different approaches are already creating challenges for businesses operating internationally.

A recent decision by the European Court of Human Rights ("ECHR") may widen the gulf between U.S. and European privacy laws. In ***Copland v. United Kingdom***,[3] the ECHR expanded the basis for protection of an employee's personal data in the workplace in Europe. The ECHR held that an employee's telephone calls and e-mails from a business are *prima facie* covered by the notions of "private life and "correspondence" under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention"). Accordingly, for the 47 nations that participate with the Council of Europe and the ECHR, such business communications are subject to reasonable expectations of privacy.[4]

---

[1] *Copland v. United Kingdom*, 62617/00 [2007] ECHR 253 (April 3, 2007)(hereinafter "*Copland*"), http://www.statewatch.org/news/2007/apr/echr-copland.pdf.

[2] The EU currently has 25 Member States: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, The Netherlands and United Kingdom.

[3] *Id.*

[4] In addition to the 25 countries that belong to the EU, the following, Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Croatia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Russian Federation, San Marino, Serbia, Switzerland, "The former Yugoslav Republic of Macedonia" Turkey

Employees' privacy rights were already heavily regulated within the European Union. For example, the EU's Data Protection Directive already provides significant protection for personal data in EU Member States. Additionally, the laws of individual Member States frequently provide significant protections for employee communications. Companies may be required to not only comply with national data protection acts, but also telecommunication regulations, labor laws, constitutional provisions, criminal laws, as well as collective bargaining agreements. The *Copland* decision, however, may create new challenges for multinational businesses operating in Europe or processing personal data from Europe.

This paper examines European data protection laws related to monitoring,[5] the *Copland* decision and the implications for companies operating in the EU and throughout Europe. This paper will also:

- Provide an analytical framework for understanding and assessing issues related to workplace monitoring in Europe;
- Examine effective management of workplace privacy risks and the risks associated with monitoring;
- Examine workplace monitoring in the EU and other jurisdictions in Europe; and
- Examine how Vontu effectively safeguards employee privacy.

Please note that this paper is the second in a series examining issues related to workplace monitoring. The first paper, entitled Protecting Confidential Information and Workplace Privacy,[6] provides a general overview focused on answering the question: "Can companies operating internationally monitor in the workplace?" The second paper, Managing Workplace Monitoring in Europe, provides an in-depth analysis focused on answering the question: "How do you monitor in the workplace in Europe?" While each of these papers can be read alone, the second paper is intended to build upon the information provided in the earlier paper.

Impact on Your Business

Why are the EU data protection laws and the *Copland* decision significant for US businesses? If your business operates in EU, compliance is a legal requirement and violations can be punished by civil and criminal penalties. Even if your company is non-European, however, EU privacy and data protection laws can still affect you in a number of distinct respects:

---

and Ukraine are participants in the ECHR and the Council of Europe. There are approximately 300 million people living in these countries.

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

[6] A copy of the paper is available on Vontu's Website at www.vontu.com.

- A EU subsidiary must comply with the privacy laws in the countries where they have operations, and as discussed below, such countries can have laws that are significantly more restrictive than those in the US and most other nations.

- The transfer of personal information can be blocked under EU law unless specific requirements are met.

- Countries around the globe are adopting laws similar to those in the EU, due in part to the global reach of the EU privacy laws.

Setting the Stage

The EU Directive and the Convention

The EU Data Protection Directive[7] ("Directive") is perhaps the best known and most influential privacy law in the world. The Directive is comprehensive, covering almost all uses of personally identifiable information by both the public and private sectors. The Directive provides a broad definition of informational privacy to include personal information processed in the workplace, including information processed by electronic monitoring technology. Ironically, the Directive itself is only a statement of EU policy—it is not the law itself.[8] Instead, the Directive requires Member States to enact national legislation to protect personal data privacy and to appoint officials to enforce these privacy rights.

Under the laws of the EU, a directive is a legislative act that requires Member States to achieve a particular result – but it does not dictate the means of achieving that result. A directive basically sets the minimum requirements for Member States. A directive can be distinguished from EU "regulations" which are self-executing and do not require any implementing measures by the Member States. This distinction is important for US companies operating in the EU and it helps explain why the privacy laws vary from one Member State to another. By leaving the Member States with a certain amount of leeway, they have adopted laws and rules that fit their particular history and culture. This means that companies must be aware of and comply with

---

[7] *Directive 95/46/EC of the European Parliament and of the Council on October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data* ("Directive.") Although the Directive was enacted in 1995, it did not become effective until 1998.

[8] There are four types of EU legislation: (a) **regulations**, which are directly applicable to Member States and require no further action to have legal effect; (b) **directives**, which are addressed to and binding on Member States, but the Member States may choose the method by which to implement the directive. Generally, a Member State must enact national legislation to comply with a directive; (3) **decisions**, which are binding on those parties to whom they are addressed; and (4) **recommendations and opinions**, which have no binding force. For more information on the sources of EU legislation, *see Research Guide: European Union Legal Materials, at* http://www.law.columbia.edu/library/Research_Guides/internat_law/eu#legislative%20process.

different legal requirements.[9] Unfortunately, many of the Member States have not adopted specific legislation or regulations to govern workplace privacy and monitoring.

The Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention") applies to a much larger number of European countries than the EU Directive. Currently, the EU is comprised of 25 countries with a population of over one-half billion people. By comparison, the Convention applies to 47 European nations with a combined population of approximately 800 million. The Convention was established after World War II to ensure that fundamental human rights are guaranteed and protected throughout Europe. Each of the 47 countries covered by the Convention are required to give effect to their national legislation in a manner that is compatible with Convention rights. This means, for example, that the privacy laws of each of the 47 countries must be interpreted in a manner consistent with the Convention.

Personal Data v. Non-Personal Data

Laws regulating the interception of communications do not typically distinguish between personal data and non-personal data. It is the act of interception or monitoring that is being regulated. If the interception involves personally identifiable information, however, then additional laws may apply. It is, therefore, important to understand what is meant by the term "personal data." For purposes of this paper, the definition contained in the Directive is used:

- **Personal data** "shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[10]

This definition covers information that many companies do not consider personal data. Equally broad is the EU's definition of the term "processing." For purposes of this paper, the definition contained in the Directive is used:

- **Processing of personal data** ('processing') "shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[11]

---

[9] In this regard, this is similar to the situation in the United States where individual states have been adopting their own privacy laws that have much in common, but may vary from state to state.

[10] Directive, art. 2.

[11] *Id.*

This paper examines monitoring or processing of employee data in the context of the workplace. Where the laws draw a distinction between monitoring of personal or non-personal data, the distinction is noted.

Employee Data v. Customer Data

This paper deals exclusively with the personally identifiable information related to employees and collected / processed in the workplace. This is important for a number of reasons. First, the purposes and justifications for monitoring in the workplace are entirely different than those that may be utilized for monitoring customer activity. Second, although the Data Directive does not distinguish between employee and customer data, European law and data protection authorities have distinguished workplace privacy issues because of the liability created by the special relationship between employer and employee. And third, the unique relationship of employer / employee creates legal rights and obligations that do not arise between company and customers. In many European countries and elsewhere, an employer may have the legal obligation to supervise and control the actions of their employees. The employer may also be liable for their employees' actions. The Article 29 Working Party[12] has stated that an employer has the right "to control the functioning of his business and defend himself against workers' action likely to harm employers' legitimate interests, for example the employer's liability for the action of their workers."[13]

The elements of control and legal liability are generally missing in the relationship between a company and its customers. Accordingly, the legal justifications for monitoring are not the same. As will be seen in the discussion of the laws of the individual Member States below, the various laws regulating workplace monitoring do not cover monitoring of customer data. Similarly, monitoring of prospective employees in a merger or acquisition would not typically fall under workplace privacy laws.

Protection of Customer Data v. Employee Privacy Rights

Privacy is not an absolute right. In both the US and EU, privacy rights must be weighed against other competing interests. To date, the Europeans have primarily viewed in terms of balancing a worker's right to privacy against the right of an employer to control the functioning of their business and to protect against liabilities that can arise out of employee actions. The EU has been very clear that with respect to workplace privacy and monitoring of employees, the employees' human

[12] Article 29 of the European Union's Data Protection Directive establishes a group of national data protection commissioners who are responsible for interpretation of the Directive. The Article 29 Working Party frequently releases opinions or other papers expounding on various aspects of privacy requirements.
[13] *See* Note 1, *supra*.

dignity trumps other considerations.[14] The following sections provide an analytical framework for determining the factors that must be considered in determining if monitoring is justified.

While the EU has viewed this issue in terms of employer rights v. employee rights, in practice there are other competing rights that must be considered. For example, employers may decide to monitor to protect the privacy rights of customers and to safeguard customer sensitive personal information from being misused by employees. The EU has not focused on the factors that should be considered in weighing the potentially competing interests in this case. Further, there is currently no EU directive that specifically governs electronic monitoring in the workplace.

Copland v. United Kingdom

The *Copland* decision involved the issue of whether U.K.'s Carmarthenshire College (the "College") violated its employee's human rights by monitoring her work e-mail, telephone calls and Internet use. Ms. Lynette Copland filed a complaint with the European Court of Human Rights (ECHR)[15] complaining that College where she worked had monitored her e-mail and telephone conversations to discover whether she was making improper use of the College's facilities for personal purposes.

The ECHR accepted the UK government's position concerning the intrusiveness and duration of the monitoring. The government admitted telephone monitoring was limited to analyzing "college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost," and lasted for "a few months" in late 1999.[16] The UK government also claimed that the Internet monitoring involved analyzing "the web sites visited, the times and dates of the visits or the web sites and their duration."[17] The government admitted that this took place during October and November 1999.[18] The government also admitted that there was no policy in force at the College at the material time regarding the monitoring of telephone, e-mail or Internet use by employees.[19]

---

[14] *See*, Article 29 Working Party Document on the Surveillance of Electronic Communications in the Workplace, 6 (May 29, 2002), *available at* http://europa.eu.int.comm/internal_market/privacy/docs/wpdcs/2--2/wp55_en.pdf.

[15] Protocol 9 of the Convention authorizes individual citizens to bring claims against their governments for alleged violations of their human rights.

[16] *Copland*, ¶ 10.

[17] *Id* .at ¶1.

[18] It is important to note that the monitoring took place before UK laws regulated such activity. The Regulation of Investigatory Powers Act (2000) and the Telecommunications (Lawful Business Practice) Regulations (2000). Additionally, the case of *Douglas v. Hello! Ltd*. [2001] WLR 992, had not been decided. The *Douglas* decision established a qualified right to privacy under English law.

[19] *Copland*, ¶14.

Based on these facts, the ECHR found that the College's monitoring violated Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention"). Article 8 provides that "Everyone has the right to respect for his private life, his home and his correspondence."[20]

Court's Reasoning

The Court's decision is based upon a number of conclusions, each of which is important to understand their scope in order to understand their impact on the data protection and privacy laws of Europe. These conclusions also identify some of the challenges that companies will face while doing business in Europe.

First, the Court determined that "telephone calls from business premises are prima facie covered by the notion of "private life" and "correspondence" for the purposes of Article 8 § 1" of the Convention.[21] The Court also found that "logically . . . e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal internet usage."[22] The ECHR concluded that the "storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1.[23]

Second, the ECHR found that even when the monitoring was limited to "the date and length of telephone conversations" and the "numbers dialed,"[24] the monitoring still gave rise to a cause of action under Article 8. Third, the ECHR discounted the College's argument that it legitimately obtained the information about the telephone calls. The Court stated: "The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8."[25]

Fourth, the Court found that it was "irrelevant" what the College did with the data. The ECHR stated: "Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings."[26]

Fifth, in the absence of a warning that her calls, e-mail and Internet usage would be monitored, Ms. Copland had a "reasonable expectation" that they would not be.[27]

Finally, the ECHR emphasized that Article 8 and its own case law require that monitoring must be conducted "in accordance with the law."[28]

---

[20] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, Rome, 4Xl.1950, art. 8.
[21] *Copland*, ¶ 41.
[22] *Id.* ¶ 41.
[23] *Id.*
[24] *Id.* ¶ 43.
[25] *Id.*
[26] *Id.*
[27] *Id.* at ¶ 42.
[28] *Id.* at ¶ 45.

Additionally, the ECHR determined that Article 8 requires domestic law to specifically state the conditions for monitoring. The ECHR found that in order to meet this requirement, the "law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort" to monitoring.[29]

Significantly, the ECHR did **not** ban the use of monitoring in the workplace. The ECHR state that it "would not exclude that the monitoring of an employee's use of a telephone, e-mail or internet at the place of work may be considered 'necessary' in a democratic society" in certain situations in pursuit of a legitimate aim.[30]

Before examining the data protection laws of individual countries, it is important to remember that the *Copland* case involved monitoring by a *public authority* (the College) with a risk of *misuse* of power.[31] Whether or not the ECHR will distinguish between monitoring by a public employer and a private employer remains to be seen.

The following sections will examine the documents issued by the Article 29 Working Party relating to workplace monitoring. We will also examine the laws and decisions of the individual Member States regarding workplace privacy. The EU Member States, however, have given little attention to the factors that should be considered when weighing the rights of customers against the competing interests of employees and employers. [32]

Managing Workplace Privacy

So, how does a company manage workplace privacy issues when the rules are varied and/or not fully established? Based upon Privacy Compliance Group's experts' experience in working with Fortune 500 companies for over a decade, it is essential to follow a process that will enable you to identify and assess the risks related to workplace monitoring. This process includes the following eight steps:

Step 1: Understand your company's data flows.

Step 2: Identify (and understand) your purposes for monitoring.

---

[29] *Id.* at ¶ 46.
[30] *Id.* at ¶ 48.
[31] *Id.* at ¶ 45.
[32] Although scant attention has been paid to the factors to be weighed when customer privacy rights are involved, as explained in this paper, using the factors established for workplace privacy in general would seem to favor allowing employers greater leeway to monitor when the purpose is specifically to protect customer data. The question is not whether or not monitoring is permitted, but rather whether or not the means for monitoring is justified under the circumstances. Utilizing monitoring technology that focuses on specific risks and uses of data will certainly increase the likelihood that monitoring will be determined to be proportional and appropriate.

Step 3: Understand the general principles underlying fair processing of personal data.

Step 4: Determine if the EU's laws apply to your company.

Step 5: Understand the EU's approach to workplace monitoring.

Step 6: Understand the EU's requirements for workplace monitoring.

Step 7: Understand the laws of the individual EU Member States.

Step 8: Implement technology that fosters compliance with legal requirements.

Each of these steps is discussed below in detail. Following these steps will provide your company's management with the information and tools necessary to manage privacy, data protection and security requirements in the EU, the US or any jurisdiction that regulates the processing of personally identifiable information.

Analytical Framework

Step One: Understand Your Data Flows

The starting point for effectively managing issues related to privacy, security and data protection is to understand your company's use of personal data and how the data flows into, through and out of your company. While this may seem like a simple first step, most companies have not mapped or documented their data flows. As a result, effective management of privacy and workplace monitoring risks is difficult, if not impossible.

In order to understand your company's data flows, there are a number of questions that should be asked, answered and documented. The information gathered from this process will enable your company to identify:

- The business requirements for the processing of personal data.
- Your company's current and future strategy and priorities, workforce composition and location, technology and other operational circumstances that impact the collection and use of personally identifiable information in the workplace.
- Specific risks associated with the collection and processing of personally identifiable data for general employment purposes or from workplace monitoring.
- The policies, procedures, laws, rules and regulations that govern the processing of personally identifiable information.
- Appropriate safeguards of employee personal data.

- Requirements for technology to enable your company to mitigate risks, safeguard data, protect privacy and confidential information and benchmark your success.
- Create and implement a risk mitigation plan.

Data flows necessarily involve business processes and technology. Since few organizations remain static, it is important to continuously evaluate your data flows. It is also essential that you choose the appropriate technology and tools to assist you in this process. Table 1 below provides a listing of the general issues along with the specific questions that should be asked and answered on an ongoing basis.

Table 1: Basic Questions of Data Flows

ISSUES	SPECIFIC QUESTIONS	INFORMATION USES
WHO?	Who is the subject of the data? Who is collecting the data? Who is accessing the data? Who is processing the data? Who is transferring the data Who is receiving the transferred data? Who is updating the data? Who is storing the data? Who is deleting or destroying the data?	Determine jurisdiction / which laws apply Determine what privacy notices / policies apply Determine what contractual safeguards must be in place Determine what physical and technical safeguards should be in place Identify ongoing risks
WHAT?	What data is being collected? What data is being processed? What data is being stored? What data is being transferred? What internal policies govern the collection and processing of the data? What laws, rules or regulations govern the collection and processing of the data??	Determine if data is sensitive / general Determine which laws / rules apply Determine what contractual safeguards must be in place Determine what physical and technical safeguards should be in place Identify ongoing risks
WHEN?	When is the data being collected? When is the data being processed? When is the data being transferred? When is the data being updated? When is the data being stored? When is the data being deleted or destroyed?	Determine if notice has been given and if so, what uses of data have been disclosed Determine which laws, rules and policies apply Determine if data is up-to-date Determine who may have obligations with respect to the data
WHERE?	Where does the data subject reside? Where is the data collected? Where is the data processed? Where is the data being transferred	Determine jurisdiction / which laws apply Determine if transborder issues must be addressed Determine if the data is being

ISSUES		
	from? Where is the data transferred to? Where is the data updated? Where is the data stored? Where is the data deleted or destroyed?	collected in the workplace
HOW?	How is the data collected? How is the data processed? How is the data transferred? How is the data updated? How is the data safeguarded? How long must the data be retained? How is the data being deleted or destroyed?	Determine if personal information is gathered from data subject, from third party or via technology Determine what contractual and other safeguards must be in place? Determine what risks are present in connection with the processing, use, transfer and deletion of the data. Determine if data is gathered through monitoring.

Step Two: Identify the Purpose for Monitoring

Identifying your purpose(s) for monitoring is required in most of the EU Member States and will almost certainly be required in order to negotiate with employees, works councils[33] and data protection authorities before monitoring can take place. Additionally, this appears to have been reinforced by the recent *Copland* decision where the ECHR held that employees have a reasonable expectation of privacy in their communications while at work until they have been notified otherwise. In the US, identification of the purpose of monitoring may not be legally required, but it nevertheless plays an important role in determining the appropriateness of who and what is monitored.

Historically, employers have asserted many good business reasons to electronically monitor in the workplace, including:

- To monitor employee productivity in the workplace;[34]

[33] Works councils are organizations representing, informing and consulting workers in companies located in more than one EU member state and with at least 1,000 employees in total, of which at least 150 are located in each of two EU member states. There is no obligation for companies or employees to establish a works council although there are procedures for workers to request one. *See*, Council Directive 94/95/EC of 22 September 1994 on the establishment of European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertaking for the purpose of information and consulting employees (1994). *Available at* http://ec.europa.eu/employment_social/labour_law/directive9445/9445euen.htm.

[34] Paul E. Hash & Christina M. Ibrahim, E-Mail, Electronic monitoring, and Employee Privacy, 37 S. Tex. L. Rev. 893, 897 (1996); Gail Lasprogata et al., Regulation of Electronic Employee Monitoring: Identifying Fundamental

- To protect against unauthorized use, disclosure or transfer of personally identifiable information on employees and customers;[35]
- To maximize productive use of the employer's computer systems;[36]
- To monitor employee compliance with employer workplace policies related to use of its computer systems, e-mail systems, and Internet access;[37]
- To investigate complaints of employee misconduct, including harassment and discrimination complaints.[38]
- 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;[39]
- To prevent or respond to unauthorized access to employer's computer systems, including access by computer hackers;[40]
- 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; [41]
- To help prepare the employer's defense to lawsuits or administrative complaints such as those brought be employees related to such claims as discrimination, harassment, discipline, or termination of employment; [42] and
- To respond to discovery requests in litigation related to electronic evidence.[43]

Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, 2004 Stan. Tech. L. Rev. 4, available at http://stlr.standord.edu/STLR/Articles/04_STLR_4.

[35] *See*, Gary E. Clayton, *Protecting Confidential Information and Workplace Privacy* (2005), available at http://www.vontu.com/offers/privacy_wp.asp.

[36] Elise M. Bloom et al., Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety, 1317 Practicing L. Inst. 303 (2002).

[37] *Regulation of Electronic Employee Monitoring*, *supra* 2004 Stan. Tech. L. Rev. 5.

[38] *Id.*

[39] Mike Consol, *Industrial Espionage: The Secret Agents of Fortune*, Bus. J. (1998), *available at* http://www.secure-data.com/art9.html .

[40] Institute for Security Technology Studies at Dartmouth College, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks, A National Needs Assessment* (2002) *available at* http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf.

[41] A. Hugh Scott, Computer and Intellectual Property Crime: Federal and State Law 141 (2001).

[42] Monique C.M. Leahy, Recovery and Reconstruction of Electronic Mail as Evidence, 4 Am Jur. 3d Proof of Facts (2002).

[43] *See Lasprogata, supra* note 9, 2004 Stan. Tech. L. Rev. 5.

[43] *Id.*

Step Three: Understand the General Principles

The US and the EU have entered into a safe harbor framework as a way to avoid interruptions in the transfer of data from the EU. Companies that certify under the safe harbor will assure that they provide "adequate" privacy protections, as defined by the Directive. Joining the safe harbor program is purely voluntary, but companies that join must agree to comply with the seven safe harbor principles.

Regardless of whether or not your company belongs to the safe harbor program, these principles underlie many of the US and EU privacy laws and serve as a useful roadmap for companies in the processing of employee data. Absent specific legislation, these principles (and the specific principles of the Directive) provide guidance for determining how to effectively protect information gathered on employees.

The seven principles require the following:

Table 2: Seven Safe Harbor Principles

Principle	Requirements
NOTICE	Companies must notify individuals about the purposes for which they collect and use information about them.
CHOICE	Companies must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for purposes other than its original purpose or the purpose authorized by the individual.
ONWARD TANSFER	Onward transfer (transfer to third parties) must be disclosed and a company must apply the notice and choice principles. Where the company wishes to transfer to a third party acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or otherwise complies with the Directive. As an alternative, the organization can enter into a written agreement with such third party requiring the third party to provide at least the same level of privacy protection as is required by the relevant principles.
ACCESS	Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete the information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individuals' privacy, or where the rights of persons other than the individual would be violated.
SECURITY	Companies must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
DATA INTEGRITY	Personal information must be relevant for the purposes for which it is to be used. A company should take reasonable steps to ensure that the data is reliable for its intended use, accurate, complete

Principle	
	and current.
ENFORCEMENT	There must be a readily available and affordable mechanism to resolve disputes and complaints and to ensure compliance with the principles.

Step Four: Determine if the EU Laws Apply to You

Determining whether or not the laws of the EU apply to your company's processing of personally identifiable information will depend upon your specific facts. As a general rule, however, if your company answers "Yes" to any of the following five questions, it is important for you to be aware of the data protection laws of the EU:[44]

Table 3: Determining if EU Laws Apply to Your Company

#	QUESTION	YES	NO
1	Does your company operate in the EU?		
2	Does your company have affiliates or subsidiaries in the EU that collect personal data?		
3	Does your company have employees residing in the EU?		
4	Does your company otherwise collect or process personal data from the EU or on EU residents?		
5	Does your company process personal data using equipment located in the EU (for other than mere transit)?		

Complexities of Workplace Monitoring in Europe

Step Five: Understand the European Approach to Workplace Monitoring

In the US, employers face a myriad of federal and state laws that protect the privacy of communications at work. These laws often limit

[44]Determining jurisdiction will depend upon a number of factors that vary by case. The issues related to determining jurisdiction are outside the scope of this paper. Internationally, there have been numerous instruments that attempt to establish standards for determining jurisdiction on various matters. In Europe, the basic instrument on jurisdiction is Regulation 44/2001 ("Brussels I") on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, O.J. (L 12)1, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_012/l_01220010116en00010023.pdf.

how and when an employer can monitor as well as what can be monitored. But generally, even without express employee consent, US employers can monitor workplace communications and activities. As a result, US employers are often advised to notify employees that they have no reasonable expectation of privacy in their communications while in the workplace or while using the employer's network or equipment. In the EU, however, data protection officials frequently state that employees do not leave their rights to privacy at home when they come to work. This has been reinforced by the *Copland* decision. As a result, European employees generally have a greater expectation of privacy than employees in the US.

In Europe, privacy is treated as a fundamental human right [45] and as such, it cannot be bargained away. This view of privacy is well founded in European law, including:

- Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: "Everyone has the right to respect for his private and family life, his home and his correspondence."[46] The Treaty Establishing the European Community requires Member States to respect the fundamental rights guaranteed by the Convention.[47]
- The EU's Charter of Fundamental Rights affirms, "[e]veryone has the right to respect for his or her private and family life, home and communications."

Most American businesses became aware of EU privacy laws after the Directive[48] became effective in 1998. The Europeans, however, have been concerned with information privacy for several decades. The formal protection of informational privacy began in the 1970s with the early stages of the computer industry. In the 1980s, the Organization for Economic Cooperation and Development, adopted its *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*.[49] In 1981, the Council of Europe adopted the *Convention for the Protections of Individuals with Regard to Automatic Processing of Personal Data.*[50] Both of these documents laid the foundation for the Directive.

---

[45] See, Barbara Crutchfield George et al., *US Multinational Employers: Navigating through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 Am. Bus. L.J. 735, 743 (2001).

[46] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, para. 1, 213 U.N.T.S. 221, *available* at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

[47] Treaty Establishing the European Community, Feb. 7, 1992, O.J. (C 224) 1 (1992), *available at* http://europa.eu.int/eur-lex/en/treaties/dat/EC_consol.html.

[48] Although the Directive was enacted in 1995, it did not become effective until 1998. While directives enact EU policy objectives, they require Member States to enact or change relevant national law to those objectives.

[49] *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. 58 (Sept. 23, 1980), available at http://www.oecd.org.

[50] *See*, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108, *available at* http://conventions/coe/int/treaty/EN/cadreprincipal.htm.

Step Six: Understand the EU's Requirements for Workplace Monitoring

The Article 29 Data Protection Working Party has adopted two principal documents relating to monitoring in the workplace. In 2001, the Article 29 Data Protection 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 its *Working Document on the surveillance of electronic communications in the Workplace*.[51] While these documents are not legally binding, they are nevertheless good indicators of how data protection issues are likely to be determined under the Directive. One reason is that the Article 29 Data Protection 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.

The main guiding principles of the Working Party can be summarized as followed:

- Employees do not lose their privacy and data protection rights at their office door.
- Any limitation on the employee's right to privacy should be proportionate to the likely damage to the employer's legitimate interests.

Employers must bear in mind the fundamental data protection principles listed in Table 4 below:

Table 4: EU Requirements for Workplace Monitoring

GENERAL PRIVACY LAW	PERSONAL DATA PROTECTION
FINALITY	Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.
TRANSPARENCY	As a very minimum, workers need to know which data the employer is collecting. Transparency is assured by granting the worker the right

[51] Article 29 Data Protection Working Party, *Working Document on the surveillance of electronic communications in the workplace*, (Adopted 29 May 2002). (*Available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf).

GENERAL PRIVACY LAW	PERSONAL DATA PROTECTION
	to access his or her personal data.
LEGITIMACY	The processing of workers' data must be legitimate. Article 7 of the Directive lists the criteria making the processing legitimate, including the following: (a) the worker has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the worker is party or in order to take steps at the request of the worker prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the employer is subject; or (d) processing is necessary in order to protect the vital interests of the worker; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the employer controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the employer or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the worker which may require protection under the Directive.
PROPORTIONALITY	The personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.
ACCURACY AND RETENTION OF THE DATA	Employment records must be accurate and, where necessary, kept up to date. The employer must take very reasonable step to ensure that data is accurate or complete, taking into account the purposes for processing the data.
SECURITY	The employer must implement appropriate technical and organizational measures at the workplace to ensure that the personal data of his workers is kept secured. Particular protections should be put in place to prevent unauthorized access.
CONSENT	The Article 29 Working Party takes the view that reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment. As will be discussed below, a number of the individual Member States specifically require employee consent before monitoring should take place.
Bottom Line: Monitoring must be proportionate to the risks confronting the employer. 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.	

Step Seven: Understand the Laws of the Individual Member States

Understanding the privacy and data protection laws of the individual Member States is important to the overall management of 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 Directive. Thirdly, in addition to variances, there is a paucity of judicial decisions, regulations or legislative guidance in a number of Member States, particularly many of the newer members. Finally, understanding these differences is essential in effectively understanding and managing risks.

At the end of this paper, a summary of the privacy and data protection laws of each Member State is provided, with particular emphasis on the law regulating workplace monitoring. It is important to remember the following statement by the Article 29 Data Protection Working Party: "In considering the question of surveillance, it must always be borne in mind that while workers have a right to a certain degree of privacy in the workplace, this right must be balanced against the right of the employer to control the functioning of his business and defend himself against workers' action likely to harm employers' legitimate interests, for example the employer's liability for the action of their workers."[52]

How Vontu Effectively Safeguards Employee Privacy

Step Eight: Implement Technology that Fosters Compliance with Legal Requirements

In developing its technology, Vontu clearly has given considerable thought to helping its customers effectively monitor the use of sensitive information while safeguarding employee privacy. Vontu's technology accomplishes this in a number of ways:

COMPLY WITH NOTICE AND POLICIES: Vontu enables companies to comply with their privacy notices and policies. Vontu does this through policy-based monitoring.

LEGITIMATE PURPOSES AND PROPORTIONALITY: Vontu ensures that data collected during monitoring is only used for legitimate purposes. Vontu 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.

---

[52] *See* n. 1, *supra*.

TARGETED MONITORING: The fair information practice principles and the principles set forth in the EU's Data Protection Directive require companies to collect data for legitimate purposes and then collect only such information that is proportional to the company's purpose for data monitoring. Vontu accomplishes this in several ways. First, Vontu safeguards employees' privacy by treating the sender's identity as "need-to-know." Second, Vontu collects only data that violates stated policy. And third, Vontu 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. Vontu has greatly reduced these risks by keeping false positives near zero.

SECURITY: Vontu provides security for the data that is collected by providing secure communications of incident data. Additionally, Vontu provides for role-based access to incident information and a complete audit trail.

ENFORCEMENT: Vontu provides an audit trail for all information gathered during monitoring. Significantly, Vontu maintains the integrity of audits by logging changes to policies and all activities taken in response to an incident.

ONWARD TRANSFER: Vontu enables its customers to restrict the transfer of personal data, thereby reducing the risks under the Directive.

ACCESS: Vontu's audit trail enables companies to easily provide individuals or work council representatives with access to specific information.

This section will examine some of Vontu's key functions that safeguard employee privacy while protecting against the loss of sensitive information.

Limits the Disclosure of Personal Information: "Need to Know"

Privacy laws and regulations apply to information that can be associated with a particular individual. If the information is anonymous or if the information is not otherwise tied to a particular individual, the risks of violating an employee's privacy rights are greatly reduced.

Vontu's Monitor detects confidential information before it leaves the network over e-mail, instant message or the Web. Vontu's Prevent stops confidential information from leaving the network and prevents internal security breaches before they occur. If a transaction is identified as a violation of the company's policies, it is cached and stored on the Vontu Monitor. This automatically triggers a transaction to Vontu Enforce by providing basic information about the policy violation. The identity of the sender, however, does not have to be disclosed. The

identity of the sender can be restricted to those the company has determined have a legitimate "need to know." Vontu can also send a message to the sender that a policy violation has occurred.[53]

Vontu can also be configured to comply with the transborder data transfer restrictions of the EU. Vontu's Monitor and Enforce can be set up so that they reside in one location within the EU. Accordingly, data collected during monitoring does not travel across national boundaries or outside of the EU.

Legitimate Purpose and Proportionality: Policy-Based Monitoring and Focus on Specific Activities

The principles of legitimate purpose and proportionality provide that monitoring is justified only if it is necessary to protect the legitimate interests of the employer and the monitoring goes no further than is necessary to meet that need. A company usually discloses the legitimate purpose in documents such as a "Network Use" policy, an "Employee Privacy" or "Customer Data Privacy" policy.

Vontu automates policy enforcement options for notification, workflow, blocking, quarantine and encryption. Vontu allows users to define and deploy data security policies based on over fifty pre-built policy templates for protecting customer data, intellectual property and company confidential information.

The focus on specific activities and policy-based monitoring helps avoid additional compliance and privacy exposures. It enables a company to provide notice of exactly what is being monitored and what is being collected. Vontu's match highlighting gives the company a clear indication of why a communication generated an incident, saving time in the incident review process and ensuring that data collected is limited to that which violates policies.

Collects Only Data that Violates Policy

Vontu monitors data flowing across a network but **only** collects data if it violates company policy. This is a significant step in protecting employee's privacy rights. Whereas some monitoring technologies capture all data — even that which does not violate policy, Vontu does not. Some of Vontu's competitors enable companies to run queries against all of the captured data in an effort to find violators. This is a clear violation of the principle of proportionality and one that Vontu does not allow.

[53] Notice to the originator of the e-mail can play an important role in establishing notice under both US and EU data privacy laws. In Europe, this can be the event that alerts an employee that his or her communication has been recorded as an incident and, therefore, triggers any rights they may have to access the data collected about the violation.

Data Accuracy and Integrity: Limits False Positives

Vontu's patent-pending technology accurately detects confidential data across all network protocols, content formats and business contexts. Accurately identifying information that violates policy is key in reducing false positives.

Vontu's Exact Data Matching delivers a high degree of accuracy on structured data. This is essential for protecting customer and employee data. Vontu's Indexed Document Matching creates "digital fingerprints" on unstructured content, enabling accuracy. And finally, Vontu's Described Content Matching uses keywords, lexicons, pattern matching (regular expression), file types, file sizes, sender, receiver and network protocol information to detect data loss incidents.

Security for Data Collected

Vontu has provided numerous features to safeguard the data that is gathered during monitoring. To begin with, the information on violations is revealed to first responders or analysts through a secure visual display. In order to protect this information during transmission, Vontu uses a secured communication channel or encrypts the information being sent. Vontu's stored (cached) documents and summary reports reside within a company's secure corporate LAN and the information is not transferred to outside parties.

Vontu also allows a customer to determine who should see specific information on incidents. The role-based access controls are important to minimize risks of the improper use of sensitive information. A customer can limit access to sensitive information or sender identity to departmental supervisors or others who should have access to such information.

Access and Enforcement: Comprehensive Audit Trail

One significant aspect of privacy protection is ensuring that an audit trail is kept of the collection and use of information. Additionally, the audit trail should keep complete records on any changes to policies as well as steps taken as a result of the incident. Vontu keeps detailed logs and accurately timestamps and records the information necessary to resolve disputes. Further, Vontu preserves evidence that may be needed for later use in the event of intentional violations.

Vontu keeps complete data on all incidents for purposes of an audit trail. Significantly, Vontu enables customers search historical data based on sender, policy, recipient and other relevant factors. This can be adjusted to comply with the EU's restrictions on how long personally identifiable data can be retained.

Onward Transfer: Limiting the Need to Transfer Data

Vontu helps its customer reduce risks from the unauthorized or inappropriate transfer to personal data collected during monitoring. Under the laws of the EU, the unauthorized transfer of personal data on residents of the EU to the US – even within the same company – can be a violation of law. Sanctions for such unauthorized transfer can include injunctions, monetary fines against the company *and* the individual employees who transferred the data and criminal penalties.

Vontu enables it customers to restrict the transfer of personal information. If data should not be transferred outside of the EU, for example, Vontu can be set up so that all components reside in one location within the EU and data will not move across national boundaries. Vontu also enables its customer to de-identify incident data so that personal information is not being transferred across national boundaries. These features are particularly important for U.S-based companies that have offices or affiliated entities located in the EU.

Grading Vontu for Effective Management of Workplace Privacy

At the outset of this paper, it was noted that effective management of workplace privacy issues requires a multi-faceted approach. Companies must educate themselves on the requirements of both US and EU laws governing workplace monitoring. Companies must also put in place effective policies and procedures to regulate monitoring and to reduce employees' expectation of privacy for workplace communications. One important element is the adoption of the Vontu solutions that will enable companies to comply with their policies, protect their sensitive information while safeguarding employee privacy. Vontu is such a technology and provides reasonable steps to protect and secure data that is gathered as a result of targeted monitoring. Vontu receives high marks for its effort to provide its customers with effective tools for safeguarding employee privacy while providing effective monitoring.

Table 5 below provides a scorecard to determine how Vontu meets the fundamental privacy principles underlying workplace monitoring. It contains a listing of the basic fair information practice principles of the US and the relevant principles from the EU as they relate to monitoring.

Table 5: Monitoring Requirements in EU

REQUIREMENT	HOW VONTU MEETS REQUIREMENT	YES/NO
Notice: Companies must notify individuals about the purposes for which they collect and use personally identifiable	Companies must notify individuals about the purposes for which they collect and use information. Although Vontu does not provide the actual notice, companies can use Vontu to ensure that monitoring takes place in compliance	**Yes**

REQUIREMENT	HOW VONTU MEETS REQUIREMENT	YES/NO
information. Notice may also require information on who is collecting the data, how it is being collected, where it will be processed and when.	with the stated purposes in the notice and, therefore, that the information in the notice is accurate. Companies most often get into trouble for stating one thing in their privacy notice and then doing something different in practice. The ability to use technology to aid in complying with a company's privacy policies is an important step in reducing privacy risks.	
Legitimate Purpose:[54] Data collection must be necessary to protect the legitimate business need of the employer. A company should carefully spell out its business reasons for data monitoring. In the U.K. for example, an employer must also conduct an assessment before monitoring in order to ensure that the steps being taken are reasonable and that the data collected will aid in achieving the objectives set by the company.	Vontu provides pre-built templates to assist customers in complying with privacy laws and best practices. Vontu provides policy-based monitoring to ensure that monitoring and data gathering only target information that violates the company's policies. These are important steps in ensuring that a company is conducting monitoring for legitimate purposes and collecting only relevant information.	**Yes**
Targeted Monitoring: The method of monitoring must be targeted to collect data for specific purposes and companies should use the least intrusive monitoring possible.	Vontu accomplishes this in a number of ways. First, Vontu only collects information that is determined to violate policy. Second, Vontu allows first responders or analysts to review incidents without revealing the sender's identity or message content. The ability to target specific data and then strictly limit who sees such data are important privacy safeguards.	**Yes**
Reasonable and Proportionate: The information gathered during monitoring must b reasonable and proportionate to the purpose for collecting.	One of the reasons that the U.K. requires an assessment prior to undertaking monitoring, is to ensure that a company understands what data should be gathered during monitoring and that monitoring is conducted in the least intrusive manner possible. Vontu aids businesses in achieving these goals by targeting only data that violates specific policies. Unlike some of its competitors, Vontu does not gather all employee communications into one large database for subsequent analysis.	**Yes**
Data Security: The	Vontu allows role-based access to incident	**Yes**

[54] "Legitimate purpose" is different than "reasonable and proportionate." The "legitimate purpose" requires a company to ensure that its purposes for data collection are allowed under relevant laws. The "reasonable and proportionate" principles ensure that a company limits the data collected to only that reasonably necessary to achieve the legal purpose for collecting data.

REQUIREMENT	HOW VONTU MEETS REQUIREMENT	YES/NO
information gathered must be protected from unauthorized use, access, alteration or destruction.	information. Vontu provides a complete audit trail of incident workflow. Finally, Vontu provides secure communication of the incident data.	
Comply with Policy: The monitoring must comply with the notice given to employees.	Vontu's policy-based monitoring allows companies to ensure that only non-compliant data is collected. This allows a company to set its policies and then feel comfortable that the monitoring is being limited to that related to the company's policies.	**Yes**
Specific Use of Data: The information gathered during monitoring must be used only for the stated purposes.	Vontu's audit trail records all workflows related to an incident — including who accessed personal information. Vontu's role-based access security enables individuals to see only what there is a "need to know."	**Yes**
Data Accuracy: The information gathered during monitoring is accurate.	Vontu's patent-pending detection technology delivers a high degree of accuracy across all types of data.	**Yes**
Onward Transfer: Transfers of personal data to third parties or to related entities must comply with the EU data protection laws.	Vontu enables its customers to restrict the transfer of personal data. If data should not be transferred outside of the EU, for example, Vontu can be set up so that all components reside in one location and data does not move across national boundaries. Vontu also enables customers to de-identify incident data so that personal information does not need to flow across national borders.	**Yes**
Access: Individuals must be given reasonable access to all personal information held about them.	Vontu's audit trail maintains a complete record if an incident workflow and all information related to the message that violated policy. Companies can easily provide employees or works council representatives with access to information on the violation.	**Yes**
Data Integrity: Steps must be taken to ensure that data is accurate and relevant for the purpose(s) for which it was collected.	Personal information must be relevant for the purposes for which it is to be used. Vontu's accuracy in monitoring data and its policy-based monitoring help ensure that the data gathered is relevant for the stated purposes.	**Yes**
Enforcement: Measures must be put in place to ensure that data is used appropriately and that the policies regarding the use of the data are enforced. Effective enforcement includes an audit trail of how data is used to ensure that individuals who violate	While Vontu will not provide the actual dispute resolution mechanism, it does provide the audit trail and records necessary for an effective dispute resolution program. Since all information related to an incident is captured and logged, along with changes to the relevant policies, employees or works council representatives can have confidence that the information is accurate and that it has not been "manufactured." If information has been inappropriately used, the Vontu audit trail will	**Yes**

REQUIREMENT	HOW VONTU MEETS REQUIREMENT	YES/NO
privacy policies are dealt with appropriately	enable companies to appropriately deal with the individuals who have violated the relevant policies.	

Table 5 provides only a starting point for you to consider before monitoring employees within the EU. Because the laws of Member States vary, it is important that you understand the laws related to each country where you are doing business. It is also very important to understand the cultural and historical perspectives of each country regarding monitoring and privacy. For many Europeans, privacy is viewed as a fundamental right that must be protected. In addition, it is important that you understand the technology that you will use to conduct monitoring, as its effectiveness and reliability can have an impact on the privacy risks you may be facing. Monitoring technology that provides safeguards to protect privacy rights of employees is an important step in managing privacy risks.

Conclusion

Monitoring has become an important part of the steps that companies must consider in order to protect their sensitive information. As discussed throughout this paper, monitoring can be used to protect the company's intellectual property as well as to protect against the leaking of customer or employee data. In order to effectively manage the risks related to the loss of sensitive data – without creating new risks by improper monitoring, companies must implement a multi-faceted program. Such a program must address the complex privacy and data protection laws of the US and the EU. An important part of any such program is the implementation of technology that provides management with an effective tool in dealing with workplace monitoring and privacy issues. Vontu technology is such a technology that should be considered by companies with international operations.

About the Author

Gary Clayton is the founder and CEO of Privacy Compliance Group, Inc., a leading privacy and data protection consulting and technology company. Privacy Compliance Group works with organizations to develop and implement effective privacy compliance programs and to develop practices and policies to comply with privacy laws around the globe.

Gary Clayton has worked with leading companies around the world and with numerous agencies of the US Government, including the Department of Homeland Security, the Department of Transportation, the General Accounting Office and the Federal Trade Commission. He has extensive experience in all aspects of privacy and has been actively involved in working with clients in over 55 countries. Mr. Clayton has worked in the EU and assisted the US Department of Commerce in negotiations with

the EU on the Safe Harbor agreement and the Department of Homeland Security in negotiations regarding access to passenger data.

Mr. Clayton is an attorney who is admitted to practice in Washington, D.C., Texas and Louisiana. He has lived and studied in Europe where he received an advanced law degree (LLM) in European and International Law from the University of Exeter, England. He has also attended the law school at the university in Grenoble, France. He is a frequent author and speaker on global privacy and data protection issues. He can be contacted at qclayton@privacycg.com.

Attachment A: Workplace Monitoring Laws in Europe

EU Countries:

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Lithuania
- Luxembourg
- Malta
- The Netherlands
- Poland
- Portugal
- Romania
- Slovakia

- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Slovenia
- Spain
- Sweden
- United Kingdom

Non-EU Countries:

- Norway
- Switzerland

Attachment A: Workplace Monitoring Laws in Europe

Austria

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Austrian constitution does not explicitly provide right to privacy. • Article 8 of the European Convention applies.	• The Federal Act concerning the Protection of Personal Data 2000[55] implements the Directive • Explicit provision regarding the use of sensitive data in the workplace	• Labor 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. • Employer must obtain agreement from Works Council even if employees have given their consent to monitoring. • The Austrian Workplace Labor Relations Act (Arbeitsverfassungsgesetz) (1974) 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.[56] The consent of the Works Council is required for "the introduction of automatic systems for the collection, processing and transmission of employee personal data."[57] 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.[58]

Bottom Line: There is little experience in Austria on workplace privacy issues. One European publication blames the lack o information on workplace privacy on insufficient support staff in the office of the data protection authority. More

[55] Federal Act concerning the Protection of Personal Data (DSG 2000), dated August 17, 1999, went into force on January 1, 2000. The DPA applies to (a) the use of personal data in Austria; and (b) the use of personal data outside Austria, provided that the data is used in another Member State for the purposes of an establishment in Austria. An English translation of DSG 2000 is *available at* http://www.dsk.gv.at/indexe.htm.

[56] ABVG, § 40(1).

[57] ABVG, § 96a(1).

[58] *Id.*

significantly, it appears that there is little dispute that employers have the right to control and regulate the production process. "This is generally deemed legitimate and works councils often fail to notice the inherent potential for surveillance."[59]

Discussion: Austria has no laws that specifically regulate monitoring in the workplace. Two laws that relate to this area may regulate electronic surveillance in the workplace. These two laws are the Labor Constitution Act of 1974, in particular sections 91 and 96. The second is the Employment Contract Law Adaptation Act of 1993. It is significant to note that since 1986, an employer has been required by law to inform the works council of employee data gathered or processed automatically, and of any processing and transfer of this data.

The 2000 Data Protection Act implements the Directive.[60] It protects the right of individuals in relation to the processing of their personal data irrespective of the mode of data processing. Individuals have the right to access, correct, delete, or keep confidential personal data. Data controllers are required to notify the data subject who has right to access the data, its origin, and the identity of any recipients. Disclosure to third parties is only allowed when the data subject gives express written permission; it is in the legitimate objective of the data controller to disclose the information; if information is not anonymous, or if it is necessary for the protection and interests of a third party. Claims against private sector data controllers can be brought under the law by an individual data subject or by the Data Protection Commission. Civil and criminal provisions apply.

Belgium

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• The principle of privacy protection is set forth in Article 22 of the Belgian Constitution: "everyone has the right to respect for his private and family life respected, except in the cases and under the conditions stipulated by law." • The right to privacy is directly binding and can be enforced by employees in the labor courts. • The law recognizes several exceptions, many of which are	• Belgium enacted the Belgium Data Protection Act (BDPA) on December 8, 1992, implemented the Directive. The law 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 BDPA seeks to regulate the collection, use and processing of personal data relating to natural persons by ensuring the data subject's right to information, access, correction or deletion, and appeal. • The DPA applies: (a) when the	• On April 26, 2002, employer and employee representatives of the National Labor Council signed national collective agreement No. 81 on the protection of the private lives of employees with respect to controls on electronic on-line communications data. • Royal Decree declared the Agreement mandatory for the private sector to govern the employee's right to privacy when electronic communications data are collected for monitoring. • Lists reasons that justify electronic monitoring • In most instances, employees must consent to monitoring. The works councils need to be

[59] *See* Eironline, European Industrial Relations Observatory Online, *Works Councils Oppose Electronic Surveillance*, *available at* http://www.eiro.eurofound.eu.int/print/1998/06/feature/at9806193f.html.
[60] An English translation is *available at* http://www.dsk.gv.at/dsg2000e.htm.

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.	processing is carried out in the context of the 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. •	informed and consulted prior to adopting monitoring technologies. • Belgian courts generally find the monitoring of e-mails to be lawful if the rules of the collective labor agreement are complied with. • September 13, 2005, a decision by a labor court in Brussels fined an employer who had fired an employee because her e-mails proved that she had been sending confidential company information to her husband who worked at a competitor. The employer in this case had not provided notice of monitoring, fired the employee on the spot and failed to confront the employee or provide her with opportunity to explain. • November 15, 2005, a labor court in Antwerp issued a similar ruling.[61] According to the labor court, e-mail surveillance is permitted only if the employees are individually and collectively notified before monitoring takes place. The employer must also have a policy on the appropriate use of network, e-mails, etc. According to the court, an employer must comply with the principle of transparency, which requires them to provide prior notification and information about e-mail monitoring on both an individual and on a collective basis. In this case, the employer had provided no such information. The employer must also comply with the principle of "finality," which allows monitoring for a limited number of purposes. If the employer does not comply with these principles, then the information cannot be used against the employer. • A labor court in Ghent issued similar rulings on May 9, 2005 and October 17, 2005.
Bottom Line: While Belgium law recognizes the rights of an employer to monitor in certain circumstances, these rights are limited and may require consent of the employees and the works council. Works councils must be informed and consulted prior		

[61] *See*, Didier Wallaert, *Belgium: Can Private E-Mails be Used in Dismissal Proceedings?*, 6 Data Protection Report 7, p. 24 (July 2006).

to the adopting of monitoring technologies. Monitoring that is targeted to specific and identifiable violations of policy – and that protect the rights of an individual to remain anonymous until a violation is detected – are the most likely to be upheld under Belgian law.

Discussion: Belgium is one of the few countries in Europe to have taken a proactive approach to clarifying the rights of an employee to privacy and the rights of an employer to monitor employees' electronic communications on employer-owned systems. Collective Agreement No. 81 provides a listing of legitimate reasons for monitoring, including:

Prevention of illegal or defamatory acts that can damage the dignity of another person;

Protection of the employer's economic, commercial or financial interests;

Security and effective operation of the company's network systems; and

Compliance with workplace policies. The Agreement also specifies conditions for monitoring, including:

Collection of data regarding Internet site visits and the number and volume of e-mail messages sent is sanctioned so long as the employee who made the visits or sent the messages is not identified.

Clear wrongdoing must be suspected before any type of individualized monitoring is permissible.

In most instances, an employee must consent to employer monitoring.

Consent must also be obtained from the employee's works council or trade union before any electronic data can be processed.[62]

Bulgaria

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Art. 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 encroachments on his honor, dignity and reputation."	• Art. 2, para. 1 of the Law for Protection of the Personal Data provides: "Personal data shall be any information related to an individual, who is identified or may be identified directly or indirectly by an identification number or through one or more specific indices, connected to his physical, physiological, genetic, psychic, psychological, mental, marital, economic, cultural or	• Bulgaria entered the European Union on January 1, 2007. No laws specifically governing workplace privacy have been enacted. Additionally, although the Commission for Data Protection has been open since it was authorized in 2002, there have been no specific guidelines regarding workplace monitoring. • Bulgarian Labor Code imposes obligations upon employees to protect confidential information of employer. The Code also imposes general obligations on the employer to protect the

[62] *See* Lasprogata, *supra* note 10, at note 158: "It is possible an employee representative body may actually consent to a type of electronic monitoring on behalf of employees, such as interception, that violates other law."

• Art. 32, para. 2 of the Constitution provides: "No one shall be followed, photographed, filmed, recorded, or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law." • Art. 34, para. 1 of the Constitution provides: "The freedom and confidentiality of correspondence and all other communications is inviolable." • Convention for the Protection of Human Rights and Fundamental Freedoms (ratified on July 31, 1992). • Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, ratified on June 7, 2002).	public identity."	employee and the employee's rights.
Bottom Line: Follow the general principles of the Directive, as there is limited legislative or other guidance on monitoring in the workplace.		
Discussion: Until specific guidance is provided, follow the general principles of the Directive.		

Cyprus

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Processing of Personal Data Law of 2001	• Processing of Personal Data Law of 2001[63] implements the Directive	• Data Protection Law does not specifically cover monitoring in the workplace.

[63] *See* Website for the Cyprus Data Protection Office, *available at* http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument.

	• The law applies to data processing carried out (a) by a data controller established in Cyprus; and (b) by a data controller not established in Cyprus but using equipment located in Cyprus for purposes other than mere transit.	• The Commissioner for Personal Data Protection is responsible for drafting codes related to the processing of personal data.

Bottom Line: Monitoring must be proportionate to the risks confronting the employer. Follow the general principles of the Directive and guidelines of the Article 29 Data Protection Working Party.

Discussion: Cyprus was one of the ten states to join the EU on May 1, 2004. To date, there has been little guidance on monitoring in the workplace.

Czech Republic

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• 1993 Charter of Fundamental Rights and Freedoms provides privacy rights, including Article 13 that states: Nobody may violate secrecy of letter and other papers and records whether privately kept or sent by post or in another manner, except in cases and in a manner specified by law. Similar protection is extended to messages communicated by telephone, telegraph or other such facilities.	• Act on Protection of Personal Data in Information Systems was adopted in 1992 • The Processing of Personal Data (Protection of the Individual Law) of 2001 implements the Directive. The 2001 law was amended in 2003, through Law No. 37(I) / 2003. • The law applies only within the Czech Republic. It applies to data controllers established in the Czech Republic and processing personal data in the Czech Republic.	• No legislation aimed specifically at workplace monitoring

Bottom Line: Monitoring must be proportionate to the risks confronting the employer. Follow the general principles and guidelines of the Article 29 Data Protection Working Party.

Discussion: Cyprus has appointed a Commissioner for Personal Data Protection who may be expected to provide guidance on monitoring in the workplace. Cyprus is likely to follow the position of the Article 29 Working Party.

Denmark

General Privacy Law	Personal Data Protection	Workplace Privacy Laws

• Danish Constitution of 1953 contains two provisions on privacy • Danish Constitution (Article 72) provides for secrecy of letters and other papers, and in postal, telegraph, and telephone matters. • § 263 of the Danish Penal Code on secrecy of mails makes it a criminal offense to open or otherwise acquire access to content of a letter or another closed message addressed to another person.	• Act on Processing of Personal Data went into effect on July 1, 2000 and implements the Directive • The Act 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.	• §263 of Danish Penal Code applies to e-mails and may be applicable in limited workplace situations
Bottom Line: Although Denmark has been fairly active in legislating privacy protections in specific circumstances, there is little specific guidance on privacy in the workplace. General principles of the Directive should be applied.		
Discussion: The Office for Personal Data Protection has a relatively small staff, but has been active in many areas of privacy. Workplace monitoring, however, is not one of the areas of activity. Monitoring in the workplace is not a widespread practice in Denmark. It is likely that Denmark will follow the opinions of the Article 29 Working Party.		

Estonia

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• The Estonian Constitution recognized 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,	• Personal Data Protection Act of 2003 [64] • Estonia Databases Act [65] primarily regulates the establishment of national databases, but does have some provisions related to the rights of individuals. • Estonia Public Information Act [66] • Surveillance Act of 1994 [67]	• No legislation specifically addressed to workplace privacy

[64] Personal Data Protection Act of 2003, English translation *available at* http://www.legaltext.ee/en/andmebaas/tekst.asp?loc=text&dok=X70030&keel=en&pg=1&ptyyp=RT&tyyp=X&query=data+protectionLink.
[65] Estonia Databases Act, English translation *available at* http://www.legaltext.ee/text/en/X1060K6.htm.
[66] Estonia Public Information Act, English translation *available at* http://www.legaltext.ee/text/en/X40095K2.htm.

telegraph, telephone or other means generally in use.	establishes the procedures for the government's conduct of surveillance. Although it deals primarily with the public/government sector, it's approach is focused primarily on the procedural aspects, rather than the establishment of individuals right of privacy. • Electronic Communications Act 2004 [68]	

Bottom Line: There is little guidance on workplace monitoring. Companies should comply with the requirements of the Directive and the Personal Data Protection Act.

Discussion: The Estonian Data Protection Inspectorate's comments in the 2005 Annual Report[69] would seem to indicate that Estonia will follow the principles and guidelines set forth by the Article 29 Working Party. Note, however, that Estonia has not signed the Convention on Protection of Individuals with Regard to Automatic Processing of Personal Data. An English version of the Inspectorate's Website is available at http://www.dp.gov.ee/index.php?id=14.

Finland

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• § 10 of Constitution provides: "Everyone's private life, honor and the sanctity of the home are guaranteed." • Protection of Privacy and Data Security in Telecommunications Act covers all communications, including e-mails and communications on	• Personal Data Protection Act of 1999 implements the Directive. • Data Protection Ombudsman enforces the Act. • The Act applies to controllers established in Finland or otherwise subject to Finnish law and to those not established in the EU but using equipment located there other than	• Protection of Privacy in Working Life – 2001 • Protection of Privacy in Working Life – 2004 • These apply to all forms of employee monitoring, regardless of form. There are specific requirements for the monitoring of emails and, in particular, personal emails.

[67] Estonia Surveillance Act of 1994, English translation *available at* http://www.legaltext.ee/en/andmebaas/ava.asp?m=022.
[68] Estonia Electronic Communications Act of 2004, *available at* http://www.legaltext.ee/en/andmebaas/ava.asp?m=022. This act deals primarily with the public administration of radio and other electronic communications; however, it does provide the owners and operators of networks certain rights to take actions to protect their networks against unauthorized use or harm.
[69] Estonia Data Protection Inspectorate's 2005 Annual Report, *available at* http://www.dp.gov.ee/index.php?id=135.

the Internet.	for mere transit purposes.	

Bottom Line: Workplace monitoring is allowed but employers must specify the purpose(s) for monitoring and involve workers or their representatives in the decision-making process. Works council's have "cooperation rights" with respect to the methods of monitoring. It will be important to identify what data will be monitored, what safeguards will be put in place to protect the data and how the workers' rights will be protected. Notice must be given before monitoring takes place. In general, monitoring of employee Internet use should not target individual employees and should be carried out only for the purposes of network security, detection, prevention and investigation of misuse.

Discussion: The Act on Protection of Privacy in Working Life (759/2004) went into effect in Finland on October 1, 2004. The law prohibits routine drug tests, places restrictions on the right of video surveillance and guarantees limited e-mail privacy for employees. The law also stipulates that the regulation of these issues is to take place through bargaining and consultation procedures at the workplace level.[70] During these consultations, employers must discuss the conditions under which e-mails may be monitored.[71] Additionally, the Act Amending Section 6 of the Act on Cooperation within Undertakings (761/2004) mandates that the following matters are covered by the cooperation procedures: "the purpose, implementation and methods used in employee monitoring performed using camera surveillance, access control and other technical methods, and the use of electronic mail and data networks."[72]

Employers have the burden of justifying the necessity to collect and use information about their employees and potential employees. Once personal information is no longer necessary, it must be destroyed or made anonymous. Generally, personal data must be collected only from individual employees. Written consent is required for processing of health data, and aptitude, psychological and drug testing may be performed only if strictly necessary and the employee has given consent. Section 3 pf the Act states that an employer is allowed to process personal data "directly necessary for the employee's employment relationship which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned." Section 3(2) of the Act states: "No exceptions can be made to the necessity requirement, even with the employee's consent."

Private E-Mails v. Employer's E-Mails: 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. The use of electronic monitoring and the purposes for monitoring are governed in part by the national labor laws, which establish participation rights of employees and their representatives. Under Finish law, the employer must specify the purposes for monitoring and the monitoring methods that will be used. Finish law also requires the employer to provide notice to all employees regarding the purposes for and means of monitoring.

E-mails retrieved, but not opened: Section 19 of the Act gives the employer "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, 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 the right. If the

[70] Finish labor law establishes a formal process for such consultations to take place. *See Act on Cooperation within Undertakings* (725/1978). An English translation is *available at* http://www.finlex.fi/en and the Act on Cooperation in Government Departments and Agencies (651/1988) *available at* http://www.finlex.fi/fi/laki/ajantasa/1988/19880651 (Finish only).
[71] Act on the Protection of Privacy in Working Life (759/2004), Section 21(1) and (2). An English translation is *available at* http://www.mol.fi/english/working/ProtectionPrivacyWorkingLife2004.pdf.
[72] Act Amending Section 6 of the Act on Cooperation within Undertakings (71/2004). An English translation is *available at* http://www.mol.fi/english/working/index.html.

message retrieval does not lead to the opening of the message, the Act requires a 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.

Opening of e-mails belonging to the employer: 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, "with the assistance of the person vested with the authority of information system administrator and in the presence of another person" 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 the content of the message to any third party.

France

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 9 of the French Civil Code provides a right to privacy. • Article 226 of the Criminal Code provides that willfully infringing someone else's privacy is a criminal offense and specifies penalties incurred for interception of correspondence.	• Law 78-17 of January 6, 1978 on information technology, files and freedoms governs collection and storage of personal electronic data.	• The French Labor Code prohibits restrictions of workers' rights and individual and collective freedoms unless it is justified by the nature of the task to be accomplished or proportionate to the desired objective. • Employers must justify monitoring. • Employees must be made aware of any monitoring. Article L. 432-2-1 of the Labor Code provides that "the Works Committee must be informed and consulted prior to any significant introduction of new technologies, when the technologies are likely to affect . . . the employees' working conditions — especially when the decisions concern means and technology allowing the control of the employees' activities." • Article L. 121-8 of the Labor Code states that "no personal information concerning an employee or a candidate for a position may be collected by a device of which the employee or the candidate would not have been informed in

		advance." • The validity of monitoring is questionable unless it is mentioned in internal policies in the form of internal rules (*règlement d'ordre intèrieur*). Employers must consult with the Works Councils before adopting and implementing these rules. • Employers must register the automatic processing of employees' data in the form of Internet monitoring with the CNIL. There is an exception to this requirement where the employer has appointed an internal data protection officer. • Transfers of personal data outside of the EU are subject to authorization and must always be registered with the CNIL. • Monitoring data generally cannot be stored for more than six months.

Bottom Line: 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. The French laws are important for those companies established in France or with offices or employees in France. The laws also apply to US companies that receive and process employee information of affiliates or subsidiaries in France. In light of the *Nikon France v. Onus* decision, businesses with operations in France should examine their policies and practices concerning monitoring of computer files and electronic communication and carefully tailor and limit monitoring to protect identified and legitimate business interests.

Discussion: In France, both the legislation and the case law provide greater privacy protections than in the U.K. The French Labor Code 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 employee's rights.

In France, all monitoring systems must be registered with the French Data Protection Authority (*la Commission Nationale de L'Informatique et des Libertes (CNIL)*) prior to implementation. The CNIL is also responsible for enforcing the privacy laws in France. The registration process requires the employer to indicate clearly the process, scope and purpose of the monitoring. Additionally, before any monitoring activities are set in place, employees must be notified of any such procedures that may affect them (Labor code, Art. L. 121-8). Such notification must be made in writing such as an internal memorandum, a statement in the company rules and regulations or in the terms of the contract of employment.

The French law also 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. (Labor Code, Art. L. 120-2), then monitoring is justified.

If the monitoring will involve personally identifiable information, making it possible to identify employees directly or indirectly, the employer must comply with the provisions of the French law on data protection and privacy.

In October 2001, France's highest appellate court held in *Nikon France v. Onos*[73] that employers do not have the right to read their employees' personal electronic mail or other personal computer files. A French business terminated an engineer's employment after a search of his e-mail and word processing files revealed that he was performing unauthorized freelance work during business hours. As the relevant computer files were marked "personal," the engineer sued Nikon saying his rights to workplace privacy and secrecy of correspondence were violated. The high court agreed, holding that an employer cannot intercept an employee's e-mail, or read e-mail marked "personal," even if the company prohibits personal use of company computers. According to the French court, reading e-mail is a "violation of the fundamental right of secrecy in one's private correspondence even when that correspondence is conducted via an employer's e-mail system and in violation of company policy.

Improper monitoring may subject an employer to civil or criminal penalties. In particular, unlawful interception of employee communications may constitute "breach of the confidentiality of personal correspondence" and may result in imprisonment of up to one year and penalties of € 35,000.

Finally, the French Supreme Court has ruled that "although the employer has the right to monitor the employee's activities during work hours, any sound or visual recordings without their knowledge, for any reason, whatsoever, constitutes illegally obtained evidence."[74] Such illegally obtained evidence cannot be the basis for an employer's disciplinary actions against an employee even if the recordings show illegal activities.

Germany

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 10 of Basic Law (the German Constitution) provides basic privacy protections for letters, posts and telecommunications.	• Germany has not enacted specific legislation on employee monitoring. • Germany has one of the strictest data protection laws in the world, both at the state (Land) and at the federal levels • Federal Data Protection Law, 2002, implements the Directive	• No law specifically governing workplace privacy; however, several laws have implications for workplace where the employer has permitted private use of e-mail and the Internet. • 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

[73] Onuf v. Nikon, *Arret* No. 4164 (Fr. Oct. 2, 2001). An English translation is *available at* http://transactionpub.metapress.com/index/BD70PA77BWC3VDPT.pdf.
[74] Cour de Cassation, Chambre sociale, *cited in* Morrison & Foerster, *Employee Privacy: Guide to US and International Law* (2007), §3.33.

	• The Law applies to data controllers located in Germany or to those located outside Germany but processing personal data in Germany.	technical equipment intended to monitor conduct or performance of employees. • For job-related e-mails, under section 4, 28 para. 1 no. 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 a 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 employee may not systematically check all e-mails of an employee in order to control the employee's performance.[75] 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 is regarded as a telecommunications service provider under the provisions of the Telecommunication Act. In such a situation, the employer is not allowed to monitor private e-mails. Any information gathered from such private e-mails could only be used for providing services.
Bottom Line: Employers can monitor e-mail communications or Internet usage if it complies with the following: (a) *Reasonableness*: e-mails may be accessed only for legitimate reasons and by means that are proportionate to the purpose for monitoring. Undifferentiated monitoring of email communications is unlikely to be permissible except in unusual circumstances. (b) *Personal Communications*: If the employer permits personal communications they cannot be monitored. Employers should consider specifically implementing a rule prohibiting private communications. (c) *Lawful Processing*: There should be an appropriate / legal basis for monitoring (e.g., consent, required by legal obligations, etc. (c) *Notice:* The employer should have a policy stating that e-mails will be only for job-related activities and that they will be monitored. Where possible, 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. (d) *Consultation with Works Council*: Under German law it may be necessary to involve the works council in the decision to employ monitoring technology and, therefore, it is important to be able to demonstrate that the monitoring is effective and is subject to safeguards that		

[75] Marc Hilber, *E-Mail Monitoring under German Law*, 6 World Data Protection Report 7, p. 22 (July 2006).

protect an employee's privacy.

Discussion: Data processing in Germany is generally governed by the Federal Data Protection Act (the "FDPA") and by the federal constitution. The FDPA applies to all types of data processing activities that are carried out in Germany, including those in the workplace. The FDPA contains no specific references to privacy in the workplace and, as a result, privacy in the workplace is to a large extent shaped by the case law of the labor courts, which have, through a series of individual cases, outlined the general principles of "employee data protection."

The employer is generally entitled to monitor the use of the company's network, the Internet and e-mail. The employer's right to monitor, however, must be weighed against the employee's privacy rights. The employees should generally be informed from the beginning of the type, purpose and extent of monitoring that will take place. (Section 81(1) German Works Constitution Act). It is sufficient to generally announce that monitoring is to be expected in the workplace. For business e-mails, monitoring is generally permissible to the full extent so that the employer is able to monitor the activities of the employees. For private e-mails, the employer is allowed to monitor the contents of private e-mails only if there is substantial suspicion of breach of contract, misuse of company assets or a criminal offense.

In Germany, the role of the works councils[76] must be considered. A works council is a legislatively created entity comprised of a group of employees with whom management of companies with over more than 150 employees must inform and consult regarding certain decision affecting employees. Not all companies have works council, but where they are established in Germany, they have the right of co-determination with respect to the introduction and use of technical systems that monitor employees. If there is no works council in a particular company, then consent must be obtained from employees before monitoring can take place.

The Labor Court of Frankfurt held in January 2002 that an employer is entitled to dismiss an employee for sending private e-mail messages only if such behavior is expressly prohibited and the employee has been given a prior warning. In addition, we understand that workplace privacy legislation is under consideration.

Greece

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• The Hellenic Constitution of 1975, as revised April 1, 2001, contains a set of fundamental rules covering privacy. [77]	• Law 2472/1997 governs the protection of individuals with respect to processing of personal data, implementing the Directive. • Law 2774/1999 governs protection of	• The Hellenic Data Protection Authority has produced a decision on monitoring in the workplace. • Data Protection Authority Decision 115/2001[78] interprets the norms laid down in laws 2472/1997[79] and 2774/1999[80] on data protection

[76] Works councils were implemented pursuant to Directive 94/45 on the establishment of European Works Councils or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees, *available at* http://ec.europa.eu/employment_social/labour_law//directive9445/9445euen.htm.

[77] English translation of the constitution is *available at* http://www.hri.org/MFA/syntagma/.
[78] English translation of Decision 115/2001 is *available at* http://www.dpa.gr/decision_eng.htm.
[79] English translation of Law 2472/1997 is *available at* http://www.dpa.gr/Documents/Eng/2472engl_all2.doc.

• The Greek constitution has several provisions on the protection of basic human rights, which includes privacy	personal data in the telecommunications sector.	for the purpose of applying them in the area of employment relationships. • Data Protection Authority Decision No. 61/2004[81] sets forth the general considerations for the monitoring of electronic communications in the workplace. • Law 1767/1988, as amended by Law 2224/1994, grants worker's councils powers to jointly decide with the employer on certain issues including surveillance.
• **Bottom Line:** 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.		
• **Discussion:** In 2004, the Hellenic Data Protection Authority issued Decision No. 61/2004[82] regarding a company's systematic and general monitoring of employee communications. The company involved was monitoring all electronic mail coming into or going out of the company' server, copying them and kept them for an "arbitrary period of time." Additionally, the company had not informed the employees that such monitoring was taking place. Finally, the company had not implemented adequate security measures or adequate policies with regard to monitoring, the use of information and company technology or a corporate e-mail policy. There were similar additional facts that no doubt influenced the Data Protection Authority: (a) Monitoring of electronic communications such as e-mail permitted insofar as it is "absolutely necessary for organizing and monitoring the performance" of the employees and business operations; (b) the monitoring is targeted and does not capture the "totality of communication data or of data of their contents; and (c) the monitoring is proportional to the risk or legitimate interests of the employer.		

Hungary

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• On July 26, 2000, the European Commission decided that Hungarian law provided an adequate level of	• Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest,[85] personal data may not be processed	• No specific legislation on workplace Privacy Compliance Group, Inc. • The Hungarian Data Protection Office sets forth guidance for monitoring at work in its

[80] *Available at* ftp://ftp.cordis.europa.eu/pub/greece/docs/n2774_1999.pdf (Greek only).
[81] English translation of Decision No. 61/2004 is *available at* http://www.dpa.gr/decision_eng.htm.
[82] *Available at* http://www.dpa.gr/Documents/Eng/Decision%2061_04.doc.

protection of personal data.[83] • 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."[84]	except upon the consent of the data subject or as allowed by law	2001 statement entitled "The employer needs the employee's consent to inspect his electronic correspondence at the e-mail address at the workplace."[86] 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.

Bottom Line: Employers should issue a clear policy stating that the computer equipment, network and communications (including e-mail, etc.) are to be used exclusively for business purposes and that they will be monitored. Employers should train staff on the policies on a regular basis and remind them of the surveillance. If feasible, a splash screen should remind them 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.

Discussion: In two opinions issued in 2001 by the Data Commissioner,[87] the conditions for monitoring of e-mails were set forth. The commissioner drew a distinction between e-mail accounts used exclusively for work purposes and those used for general purposes. In cases where e-mail use 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 thee conditions, "he will have controlled data just as illegally as if he tapped the employee's phone lines.

Ireland

[83] Article 29 Working Party Opinion of September 7, 1999 on the protection of individuals with regard to the processing of personal data, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp24en.pdf.
[84] *Id. citing* an English translation provided by the Government of Hungary.
[85] English translation is *available at* http://www.privacy.org/pi/countries/hungary/hungary_privacy_law_1992.html.
[86] English translation is *available at* http://abiweb.obh.hu/dpc/index.php?menu=cases/DP/2001&dok=20010423.
[87] Opinion of April 2001, *available at* http://abiweb.obh.hu/dpc/index.php?menu=cases/DP/2001&dok=20010423. Opinion of August 2001, *available at* http://abiweb.obh.hu/dpc/index.php?menu=cases/DP/2001&dok=20010830.

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Irish Constitution does not specifically provide the right of privacy although several cases have implied this right.	• Data Protection Act 1988 [88] (amended April 2003)[89], implements the Directive	• No specific legislation. • The Data Protection Commissioner has issued guidance notes on the monitoring of staff that specifically acknowledges that organizations have a legitimate interest to protect their business, reputation, resources and equipment and that monitoring may be a legitimate means of achieving this.

Bottom Line: In the absence of a clear policy, employees are assumed to have a reasonable expectation of privacy in the workplace. Employers should carefully craft policies to disclose what monitoring will take place and to ensure that the information is adequately safeguarded. 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. Employees should be given access to their information.

Discussion: In January 2006, Ireland's Data Protection Commissioner issued "Guidance Notes" on the monitoring of staff in the workplace.[90] This document sets forth the basic guidelines for employers who wish to monitor within Ireland, including the following: (a) employers have a legitimate interest in protecting business, reputation, resources and equipment; (b) these interests do not take precedence over the principles of data protection; (c) monitoring must comply with the requirements for transparency; (d) monitoring must be carried out in the least intrusive way possible; (e) the principal of proportionality must be followed; and (f) any personal information gathered in the course of monitoring must be adequate, relevant and not excessive and retained for only as long as necessary for the purpose for which the monitoring was justified.

The Data Protection Commissioner's Guidance Notes includes a template for and acceptable use policy that the Commissioner suggests companies to use in relation to e-mail and the Internet.

Italy

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Italian Constitution[91] has several limited provisions	• The Italian Personal Data Protection Code implements the	• The Italian Personal Data Protection Code brings together all of the various laws, codes

[88] *Available at* the Irish Data Commissioner's Website http://www.dataprivacy.ie/viewdoc.asp?Docid=64&Catid=47&StartDate=1+January+2006&m=l.
[89] *Available* at the Irish Data Commissioner's Website, http://www.dataprivacy.ie/viewdoc.asp?Docid=68&Catid=47&StartDate=1+January+2006&m=l.
[90] *Available at* http://www.dataprotection.ie/docs/Guidance_Notes__Monitoring_of_Staff/208.htm.
[91] An English translation of the Italian Constitution is *available at* http://www.oefre.unibe.ch/law/icl/it00000_.html.

related to privacy – although none specifically apply to the workplace.	Directive and applies to workplace monitoring.[92]	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 implemented 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." • Section 134 relates to video surveillance, but only notes that the Italian Guarantee will encourage the adoption of a code of conduct for conducting such monitoring. • *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. 300/70) 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. • On March 10, 2007, the *Garante*, Italy's data protection authority, issued a guidance paper

[92] Italian Data Protection Code, Legislative Decree No. 196 of 30 June 2003. An English translation is *available at* http://www.garanteprivacy.it/garante/document?ID=311066.
[93] Karin Retzer and Teresa Basile, *Italy's DPA Publishes New Rules on Monitoring Employees*, (May 2007), http://www.mofo.com/docs/pdf/ItalyDPA.pdf.
[94] *Id.*
[95] *Id.*

		to help employers monitor in a way that complies with the requirements of the EU Directive and Italian law.[93] • The *Garante* has ruled out any systematic and constant monitoring through software or hardware to the extent that it is aimed at "directly controlling" employees' activity. Information obtained through systematic monitoring is unlawful and cannot be used by the employer in court. Employers may only monitor in compliance with the data protection principles: (a) necessity; (b) finality; (c) transparency; (d) proportionality; (e) accuracy and retention of data; and (f) security. [94] • The *Garante* has set out specific notice requirements [95]that employers must meet in order to legally monitor.

Bottom Line: Monitoring is legal but it must comply with the data protection principles. Systematic and constant monitoring is not permitted and cannot be used as a basis for disciplinary actions against employees. Employers may only monitor in compliance with the data protection principles: (a) necessity; (b) finality; (c) transparency; (d) proportionality; (e) accuracy and retention of data; and (f) security.

Employers should adopt a policy describing the monitoring that will take place and describing the purposes for monitoring. Monitoring should be targeted to communications that violate specific policies. Use of the data should be limited and the data 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 (9) 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 is periodically deleted for appropriate reasons.

Discussion: In January 2002, the Italian Data Protection Commission (DPA) decided that employees generally have the right to access any document containing their personal data in the possession of their employer. Italian privacy law grants individuals the right to access personal data collected about them. An employee accordingly requested from his former employer all e-mails containing his professional evaluations, and appealed to the DPA after the employer refused to disclose these materials. The DPA ruled that companies are required to extract from documents in their possession (other than personal communications) all personal information concerning the requesting employee and to communicate such information to the employee in an easily understandable form.

Latvia

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Art. 96 of the Latvian constitution provides: "Everyone has the right to the inviolability of a private life, place of residence and correspondence." • Arts. 12 of the Universal Declaration of Human Rights protects privacy. • Latvia is a signatory to the Convention for the Protection of Human Rights and Fundamental Freedoms	• Personal Data Protection Law implements EU Data Protection Directive.	• The Latvian Data State Inspectorate (DSI) issued an opinion (2005) regarding an employer's right to monitor e-mail communications. DSI's advice complies with the EU Data Protection Directive and mandates that the employer develop and implement an "Information Security Policy" that should be in force throughout the company, binding on all employees and inform employees that monitoring will take place, how information will be used, who will have access and how the information will be used. The policy should make it clear that the network, e-mal and Internet are to be used only for business purposes.

Bottom Line: Employer must develop and implement an "Information Security Policy" that should be in force throughout the company, binding on all employees and inform employees that monitoring will take place, how information will be used, who will have access and how the information will be used. The policy should make it clear that the network, e-mal and Internet are to be used only for business purposes

Discussion: In addition to following the above requirements, the employer must be certain that there is no agreement between employer and employees / labor union that would restrict the ability to monitor use of computers, e-mail, etc.

Lithuania

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Art. 22 of the Lithuanian constitution provides: "(1) The private life of an individual shall be inviolable. (2) Personal correspondence, telephone conversations, telegraph messages, and other intercommunications shall be inviolable. (3) Information	• Law on Legal Protection of Personal Data enacts data protection obligations under the EU Data Protection Directive. • Law on Electronic Communications protects the confidentiality of electronic communications. Section 63 protects the confidentiality of communications over electronic communications networks and	• No laws specifically addressing workplace monitoring.

concerning the private life of an individual may be collected only upon a justified court order and in accordance with the law. • (4) The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life, and from encroachment upon their honor and dignity."	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 situations 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."	

Bottom Line: Follow the general principles of the Directive, as there is limited legislative guidance on monitoring in the workplace.

Discussion: Lithuania joined the European Union in 2004. Lithuania 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 should provide information on purpose of monitoring.

Luxembourg

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 29 of the constitution protects secrecy of correspondence	• Law of 2 August 2002 implements the Directive	• 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' behavior and performance at their work stations.

Bottom Line: Follow the general principles of the Directive, as there is limited legislative guidance on monitoring in the workplace.

Discussion: 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 should provide information on purpose of monitoring.

Malta

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Art. 32 of the constitution provides for protection of "private life". • Art. 41 of the constitutions provides for protection of "correspondence".	• Data Protection Act (CAP 440) ACT XXVI of 2001, as amended by Act XXXI of 2002.[96]	• The Data Commissioner's Website provides the following statement: "Surveillance methods involving the collection or otherwise processing of personal data, is another sector where guidelines will be issued by this Office."[97] To date, however, no such guidelines have been issued. The Commissioner's office noted only 3 surveillance-related complaints during 2005 and none during 2004.[98]

Bottom Line: Follow the general principles of the Directive, as there is limited legislative or other guidance on monitoring in the workplace.

Discussion: The Data Commissioner's Website indicates that the Commissioner's office will be issuing guidance on monitoring. To date, however, there is almost no guidance. Accordingly, companies considering workplace monitoring should follow the general principles of the Directive and the Article 29 Working Party.

The Netherlands

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 10 of the Dutch Constitution states that all citizens are entitled to respect of their personal privacy (§10)[99]	• Personal Data Protection Act of July 6, 2000 [100]implements the Directive	• The Dutch 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

[96] Data Protection Act of 2001, *available at* http://www.dataprotection.gov.mt/dbfile.aspx/DPA.pdf.
[97] *See* http://www.dataprotection.gov.mt/article.aspx?art=117.
[98] *See* Data Commissioner's Annual Report for 2004, *available at* http://www.dataprotection.gov.mt/dbfile.aspx/Annual%20Report%202004.pdf and the Annual Report for 2005, *available at* http://www.dataprotection.gov.mt/dbfile.aspx/Annual%20Report%202004.pdf.
[99] An English translation of the Dutch Constitution is *available at* http://www.oefre.unibe.ch/law/icl/nl00000_.html.
[100] An English translation of the Personal Data Protection Act is *available at* http://home.planet.nl/~privacy1/wbp_en_rev.htm.

• Article 13 guarantees privacy of correspondence, telephone and telegraph communication		personal data that are processed within the scope of the employment relationship." [101] • "Checking on e-mail is not prohibited."[102] 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 Data Protection Authority has set forth the following 17 "rules of thumb": (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. Which software may be used for this; (5) As far is 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 behavior 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 a control mechanism 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. • The Works Councils Act (§27.1), gives works council the right of consent (a kind of veto

[101] Dutch Data Protection Authority Website, Working Well in Networks, *available at* http://www.dutchdpa.nl/indexen/en_ind_arb.shtml?refer=true&theme=purple.
[102] *Id.*, http://www.dutchdpa.nl/downloads_av/AV21.pdf?refer=true&theme=blue.

		power) when the employer intends to introduce, change or abolish a rule on: the collection and processing of employees' personal data; or facilities aimed at, or suitable for, the observation or control of employees' presence, behavior or performance.

Bottom Line: 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.[103]. 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."[104] Employees should consider how to comply with the 17 rules of thumb listed above.

Discussion: Employers should carefully consider how to comply with the 17 rules of thumb provided by the Dutch Data Protection Authority. An employer should document its assessment of the 17 rules of thumb and why (or why not) they apply to the facts and circumstances related to your workplace. Employers should consider conducting and/or following an assessment based upon the Privacy Audit Framework that was issued in 2001.[105]

Poland

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Polish Constitution[106] recognizes the right to privacy. Article 47 provides legal protections to a citizen's personal and family life. Article 51 limits the circumstances in which the state can gather personal data and confers specific rights upon citizens, such as the right of access.	• Act on Personal Data Protection amended 2004 [107] • The Act applies not only to organizations that are "established" in Poland, but also to individuals that are "domiciled" there. • Poland has implemented the Regulation of April 29, 2004, by the Minister of Internal Affairs regarding the security of personal information that requires proper	• No legislation specifically addressing workplace monitoring. • The General Inspector for the Protection of Personal Data has not provided guidance on the issue of workplace monitoring. • Poland has not signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

[103] *Id.*
[104] *Id.*
[105] "Privacy Audit Framework under the new Dutch Data Protection Act (WBP)," Version 1, April 2001 is *available at* http://www.dutchdpa.nl/downloads_audit/privacyauditframework.pdf?refer=true&theme=purple.
[106] English translation of the Polish Constitution is *available at* http://www.oefre.unibe.ch/law/icl/pl00000_.html.

	management of personal data, including employee data.[108]	

Bottom Line: Follow the general principles of the Directive, as there is little or no guidance or legislation on monitoring in the workplace.

Discussion: The General Inspector for the Protection of Personal Data has issued a limited number of decisions since its creation in 1998.[109] Based upon the decisions to date, however, it appears that Poland will generally follow the guidelines and recommendations provided by the Article 29 Working Party.

Portugal

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Portuguese Constitution[110] recognizes rights to personal identity, privacy of correspondence and other means of private communication and data protection	• Law 67/98 of 26 October 1998[111] on Personal Data Protection implements the Directive	• The Portuguese Data Protection Office has issued recommendations on the monitoring of employees in the workplace.[112] 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

[107] Act on the Protection of Personal Data of 29 August 1997 (Journal lf Laws No. 101, item 926, as amended). An English translation is *available at* http://www.giodo.gov.pl/data/filemanager_en/61.doc.

[108] §§ 3 and 4 of the Regulation of April 29, 2004, by the Minster of Internal Affairs and Administration as regards personal data processing documentation and technical and organizational conditions, which should be fulfilled by devices and computer systems, used for personal data processing (Journal of Laws No. 100 item 1024). An English translation is available at http://www.giodo.gov.pl/144/j/en/.

[109] *See* the General Inspector's Website at http://www.giodo.gov.pl/138/j/en/.

[110] An English translation of Poland's Constitution is *available at* http://www.oefre.unibe.ch/law/icl/po00000_.html.

[111] An English translation of the Personal Data Protection Act is *available at* http://www.oefre.unibe.ch/law/icl/po00000_.html.

[112] "Recommendations of the Portuguese Data Protection Authority Regarding the Monitoring of Employees at the Workplace: Phone Calls, E-Mail, Internet Access" (English), available at http://www.cnpd.pt/english/bin/guidelines/privacyworkplace2002.HTM.

		employees. • 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 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 an 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.
Bottom Line: Employers must adopt a clear policy on the use of company communications equipment and discloses to the employees that monitoring will take place. Employers must provide information to the employees on the 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 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 may block the e-		

mails before it departs the company's network and/or ensure that the employee receives immediate notice. An audit trail should be kept.

Discussion: Companies considering monitoring in Portugal should carefully read the DPA's recommendations and consult with employees regarding the technology and means of monitoring. Companies should follow the general guidelines of the DPA's office, the Directive and the Article 29 Working Party. Technology that is used to monitor should focus on specific violations and minimize the amount of data that is captured or disclosed to the employer. Where possible, employee consent should be obtained after consultation with employees and their representatives.

Romania

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 26(1) of the Romanian Constitution provides: "The public authorities shall respect and protect the intimate, family and private life."	• Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and Free Circulation of Such Data and subsequent amendments implement the EU Data Protection Directive. • Law No. 506/2004 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector provides for the confidentiality of communications on "public electronic communications networks and publicly available electronic communications services." Art. 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.	• Romania has not enacted legislation specifically addressing workplace privacy.

Bottom Line: Follow the general principles of the Directive, as there is little or no guidance or legislation on monitoring in the workplace.

Discussion: Romania became a member of the European Union on January 1, 2007. Romania's National Supervisory Authority for Personal Data Processing was established in 2005 by Law No. 102/2005.

Slovakia

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• The 1992 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	• Protection of Personal Data Act of 2002[114]	• No legislation specifically directed to regulating workplace monitoring.

[113] An English translation is *available* at http://www.legislationline.org/upload/legislations/0f/f8/3d4977d97d4d8fe818a162fe2c0e.htm.
[114] An English translation is *available at* http://www.privireal.org/content/dp/documents/SlovakiaAct428_2002%20_2005_PersonalData.pdf.

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."[113]		

Bottom Line: Follow the guidelines of the Article 29 Working Party and the requirements of the Directive. Coordinate with the Commissioner for the Protection of Personal Data in Information Systems.

Discussion: For additional information, *see* Website of the Office of Personal Data Protection, http://www.dataprotection.gov.sk/buxusnew/generate_page.php?page_id=93.

Slovenia

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 35 of the 1991 Constitution provides: "The inviolability of the physical and mental integrity of every person, his privacy and personality rights shall be guaranteed." • Slovenia has ratified the Convention for the Protection of Individuals with Regard to	• Personal Data Protection Act[115] has been noted as "deficient" by the EU Commission because of the wording of its Personal Data[116] Protection Act, which applies by virtue of where the data subject is located. As a result, every individual in Slovenia (whether a Slovenian or non-Slovenian citizen) is protected under the act, wherever his or her data is processed in the world.[117]	• Annual Report 2004 [118] provides a discussion of the various initiatives by Slovenia, but does not discuss workplace privacy or monitoring. • No specific law dealing specifically with workplace monitoring.

[115] An English translation is *available at* http://www.privacyexchange.org/legal/nat/omni/slovenia.html.
[116] The First Report on the implementation of the Data Privacy Directive 995/46/EC) — Commission of the European Communities COM (2003) 265, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT.
[117] Article 6 of the Personal Data Protection Act states: "Any individual, regardless of their nationality and place of residence, shall be guaranteed personal data protection on the territory of the Republic of Slovenia."
[118] *Available at* http://www.dataprotection.gov.sk/buxusnew/docs/status_report_2004.pdf.

Automatic Processing of Personal Data.	• Article 3 of the Personal Data Protection Act provides: "Personal data may only be processed if data-processing is determined by law or if the database administrator has acquired the written consent of the individual."	

Bottom Line: Obtain written consent or acknowledgement from employees before monitoring takes place. Comply with the requirements and guidelines set forth by the Article 29 Working Party.

Discussion: Slovenia's legislation exceeds the requirements of the Directive in a number of areas. There is no legislation, however, specifically dealing with workplace monitoring and privacy.

Spain

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Article 8 of the Spanish Constitution provides the right to personal and family privacy. • Article 167 of the Penal Code prohibits the unlawful interception of communications. • Note, however, that neither of these explicitly apply to workplace monitoring.	• Organic Law 5/1992 on the Regulation of Automatic Processing of Personal Data • Organic Law 15/1999 on the Protection of Information of a Personal Nature implements the Directive • Royal Decree 428/1993 created the Spanish Data Protection Agency • Royal Decree 994/1999 regulates the security of personal information contained in electronic / automated files.	• Article 64 of the Workers' Statute established the right of works councils to issue a report on the introduction of monitoring • Articles 5 and 20 of the Labor Act give employers the right to direct the labor activity and to monitor or supervise employees' work-related obligation – but these rights must not impinge the dignity of the workers. • 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.

Bottom Line: There has been conflicting court decisions in Spain. Employers should have a policy, stating the right to monitor, and provide notice to employees. Employers must not monitor communications with a labor union.

Discussion: There are conflicting opinions in Spain. If employers are to monitor, it is recommended that the following steps be followed: (1) Establish a policy and set forth the right to monitor; (2) provide a 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 the e-mails are the property of the company; (4) employers should focus their monitoring on violations or policy; (5) provide notice to union representatives or works councils; and, (6) keep an audit trail and consider having employee representative or third party participate / observe the process to ensure it is conducted fairly.

Sweden

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Swedish constitution[119] provides for the privacy of correspondence and the confidentiality of communications	• Data Protection Act of 1998[120] implements the Directive. It is supplemented by the Personal Data Ordinance.[121]	• Monitoring of e-mails is regulated by the Penal Code and the Data Protection Act • Data Commissioner's Office has published a checklist that should be followed.

Bottom Line: The Swedish Data Commissioner acknowledges that there is little experience or guidance on workplace monitoring. In Sweden, an employer has the right to monitor. Employers should follow the checklist provided by the Data Commissioner's office.

Discussion: The Swedish data protection office has published a "checklist"[122] that provides the following guidance:

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.

If the employer carries out some kind of checks concerning the employees' use of the Internet and e-mails, this must be clearly evident from regulations and information provided. It should be made clear how the check is carried out.

If the employer may go through the contents of an employee's private e-mail messages, this must be made clear by regulations and information provided.

Employers should make clear what kinds of measures would be taken if employees violate the policies.

Employers should make it clear how long it will keep data that is the basis of the checks of the employee's use of the Internet and e-mail.

[119] An English translation of Sweden's Constitution is *available at* http://www.oefre.unibe.ch/law/icl/sw00000_.html.
[120] An English translation of Sweden's Data Protection Act is *available at* http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf.
[121] An English translation of Sweden's Personal Data Ordinance of 1998 is *available at* http://www.sweden.gov.se/content/1/c6/01/55/42/b33e1fd3.pdf.
[122] An English translation is *available at* http://www.datainspektionen.se/pdf/ovriqt/checklist_monitoring_worklife.pdf (last visited August 15, 2006).

United Kingdom

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Interception or review of employee communications as well as the processing of personal data, is covered by the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practices) 2000.	• Data Protection Act 1998 [123] implements the EU Data Protection Directive • The Regulation of Investigatory Powers ("RIP") Act of 2000 [124] regulates the monitoring or interception of e-mails and other forms of communication. • The Telecommunications (Lawful Business Practice)(Interception of Communications Act) Regulations 2000 regulates the interception of communications, including e-mails.	• Extensive guidance provided by the UK Information Commissioner's office, including the Employment Practices Data Protection Code.[125] This code sets forth specific requirements and procedures that must be followed before monitoring can take place. • Impact assessment must be performed before monitoring takes place.

Bottom Line: A detailed impact assessment must be performed to document a business need for monitoring, and the method of monitoring must be targeted and the least intrusive possible. Written notice must be provided to employees providing clear information on how monitoring will be conducted, what information will be collected and the reason for the monitoring.

Discussion: In the United Kingdom, workplace monitoring is regulated by the **Data Protection Act of 1998** as it generally involves the processing of personal data. However, the Information Commissioner has set out detailed guidance for companies as to how the legislation applies to workplace monitoring. The Information Commissioner's office has published its **Employment Practices Data Protection Code** to regulate workplace monitoring. The Code expressly recognizes the need to "strike a balance between a worker's legitimate right to respect for . . . private life and an employer's legitimate needs to run its business." Under the Code, employers are required to carry out an impact assessment to establish whether any planned monitoring is necessary to address a legitimate business need, and goes no further than is necessary to meet that need.

The UK Information Commissioner is responsible for enforcement of the Employment Practices Data Protection Code and the Data Protection Act of 1998. This does not prevent individual employees or potentially other interested parties from pursuing claims against employers who do not comply with the law. Any company that collects or processes personal information on employees located in the U.K. should carefully review and understand the Information Commissioner's codes.

---

[123] *Available at* http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm.
[124] *Available at* http://www.opsi.gov.uk/Acts/acts2000/20000023.htm.
[125] *The Employment Practices Code, available at* http://www.ikco.gov.uk/cms/DocumentUploads/employment_practices_code.html; *see also, The Employment Practices Code Supplementary Guidelines, available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html.

The UK Information Commissioner's Employment Practices Data Protection Code and Supplementary Guidance discusses steps hat companies must follow if they are to engage in workplace monitoring. (1) Conduct the assessment required by the Code; (2) Adopt and publish a policy and notices that are known and understood by workers; (3) Follow the rule of proportionality and minimize the monitoring or target actions that violate specific policies; (4) limit the access to monitored information to only those personnel who have a need to know; (5) ensure that information is kept securely and not improperly disclosed; (6) comply with the requirements of the Data Protection Act, the Lawful Business Practices Regulations, the Code and Guidelines; (7) **use sophisticated automated monitoring systems to assist data protection compliance.**[126] In addition, business should ensure that employees continue to have secure lines of communication for the transmission of sensitive information from the worker to a health advisor or for trade union communications that will not be monitored.

The Information Commissioner seems to draw a distinction between surveillance where humans "open" e-mails or other communication and the use of monitoring technology to determine if the contents of an e-mail violates policy. As noted above, the Information Commissioner has suggested that companies considering monitoring implement appropriate technologies that can assist in compliance.

Non-EU European Countries

Norway

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Norwegian Constitution[127] does not explicitly provide right to privacy. • Norwegian courts have established a fundamental legal principle of 'protection of personal integrity.' The principle is similar to privacy principles in other European nations.	• The 2000 Act relating to the Processing of Personal Data[128] governs personal privacy.	• The Act relating to Workers Protection and Working Environment implies that monitoring of employees may not be carried out if such activity breaches the provisions of the Act by subjecting employees to health-related hazards. • Norwegian law requires employers to control and monitor working life for permissible purposes.

Bottom Line: Although Norwegian law authorizes employers to control and monitor employees / working life, follow the general principles of the EU Data Protection Directive.

[126] *Id., The Employment Practices Code Supplementary Guidance*, § 3.2.3, p. 35.
[127] An English translation of the Norwegian Constitution is *available at* http://www.oefre.unibe.ch/law/icl/no00000_.html.
[128] An English translation of the Processing of Personal Data Act is *available at* http://www.datatilsynet.no.htest.osl.basefarm.net/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf.

Discussion: There is limited guidance on the use of surveillance due to the limited use of workplace monitoring.

Switzerland

General Privacy Law	Personal Data Protection	Workplace Privacy Laws
• Swiss Constitution[129] recognizes privacy and the secrecy of communications • Individual Cantons have passed privacy legislation • The EU has determined that Switzerland provides "adequate protection"	• Federal Data Protection Act became effective 1993 • Ordinance on the Federal Law of Data Protection	• Section 328 of the Code of Obligations establishes general conditions for workplace monitoring • The Federal Data Protection and Information Commissioner has issued guidance on Spy Programs[130] that are described as surveillance without the knowledge or consent of the employee or third party. • The Commissioner has made the following statement: "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."[131]

Bottom Line: 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.

In order to avoid privacy problems, employers should consider setting up employee e-mail accounts in such a manner as to

[129] An English translation of the Swiss Constitution is *available at* http://www.oefre.unibe.ch/law/icl/sz00000_.html.
[130] Switzerland Federal Data Protection and Information Commissioner, *Spy Programs from a Data Protection Standpoint*, *available at* http://www.edoeb.admin.ch/dokumentation/00445/00509/00512/00803/index.html?lang=en.
[131] *Id.*

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: hans.meier@companyname.ch or hans.meier@sales.companyname.ch (as possibly indicating personal use is permissible), on the one hand, and info@companyname.ch, sales@companyname.ch, or salesmanager@companyname.ch (as indicating business purposes only and thus avoiding privacy issues).

Note: 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." [132] 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.")[133]

Discussion: The Swiss Data Protection and Information Commissioner has issued the following guidance on "spy programs: "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." [134]

---

[132] Switzerland Federal Data Protection and Information Commissioner, *E-Mail Management during Absences and on Leaving the Company*, http://www.edoeb.admin.ch/dokumentation/00445/00509/00512/00804/index.html?lang=en.

[133] *Id.*

[134] Switzerland Federal Data Protection and Information Commissioner, *Spy Programs from a Data Protection Standpoint, available at* http://www.edoeb.admin.ch/dokumentation/00445/00509/00512/00803/index.html?lang=en.

EU Countries:

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- The Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

Non-EU Countries:

- Norway
- Switzerland

^**Back to Table of Contents**^