SAFETICA – ETHICS, LEGAL USE, AND THE MAIN ADVANTAGES OF THE SOFTWARE FOR CLIENTS' EMPLOYEES

www.safetica.com

safetica®

EXECUTIVE SUMMARY

Any activity-tracking, data protection solutions raise concerns. One must realize that implementing them will benefit both the company and its employees, assuming that all legal requirements pertaining to the monitoring of people and data are met. The law also imposes requirements on protecting private information.

HOW CAN SAFETICA BENEFIT YOUR EMPLOYEES?

Safetica is a solution that protects companies and their employees from errors caused by the human factor. It helps employees to avoid mistakes that might be made during handling company data, thereby help them avoid being fired. It also protects the company – the employer – from large financial losses and damage to reputation caused by leakage of sensitive data. The software helps achieve conformance with personal data protection laws and facilitate a correct way of handling the personal information of employees.

What Will Never Happen to You if You Use Safetica?

- You send out an e-mail with sensitive information about your business to your competitor by accident
- A ready-to-use database of customers ends up in the hands of a thief who steals your laptop from your car
- Leakage of data from your company exploited by your competitor gets you fired, as your employer is forced to make lay-offs on account of losing clients to the exploiter
- An unauthorized person gets their hands on your salary information and spreads it to the rest of the company
- Your division scores bad results on its performance review, as some of your colleagues prefer playing PC games, facebooking, instant messaging, or online shopping to doing actual work
- You can't work as the PC network has been infected by computer viruses let in by your colleague who has been browsing inappropriate websites
- Instead of dispensing bonuses, your employer has to pay tens of thousands of dollars in fines to the government for failing to meet the legal requirements on the protection of personal data

Remember: By using Safetica, your employer is protecting you, your personal data, and your job.

MONITORING, PROTECTION OF DATA, AND THE LAW

Protecting company data is not just a legitimate concern of company managers; if the data contains personal information on customers or employees, it becomes the company's legal responsibility in most countries. One way to meet this responsibility is to design company ISMS (Information Security Management Systems) in compliance with the standards prescribed by the ISO/IEC 27000 family. These standards are applicable to companies of all sizes all over the world, and they are gaining wider and wider acceptance due to efforts to build trust and comply with laws.

Besides this data protection responsibility, the Safetica monitoring functions in particular are subject to laws on the protection of personal rights and freedoms. Along the lines of where the rights of employees and the employer meet, certain adjustments must be made so as to really ensure that both company property and employee privacy rights are protected. The concrete requirements may vary depending on your location.

Know Your Rights

Safetica Technologies s.r.o. offers a complete internal security solution and advice on how to use this solution so that either party's rights are respected. Each company, however, bears full responsibility for using Safetica in compliance with local laws. Make sure to learn about your rights, and speak to your employer if you have questions.

Data collected from monitoring are also subject to protection, and you can set detailed access rights on them (i.e. and IT technician will set the software up and turn it on, but he will not view your activity log). Moreover, the individual monitoring functions of Safetica work independently and you can turn them off selectively.

LAWS IN DIFFERENT COUNTRIES

The legal obligation to protect data is the strongest in the **United States**. Systems that process financial information are particularly obligated to ensure data security in accordance with the Gramm-Leach-Bliley Act (GLBA); systems processing medical information are obligated to do so in order to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

The Electronic Communications Protection Act governs monitoring in the workplace. To meet its requirements, employees' consent to monitoring has to be gained, or the "provider" and "business use" exceptions may be argued instead, which limit communication monitoring to infrastructures owned by the company or on messages that are related to work done for the company.

In **Europe**, the laws emphasize the rights and freedoms of employees much more, and obtaining the employee's consent where the employer intends to process personal information or conduct monitoring is mandatory. Individual European countries where the EU Directive 95/46/EC on the protection of private information has been implemented add further legal requirements that must be met (e.g., ensuring data and system security in systems processing personal data; conditions for transfers outside the EU; sending notifications to local authorities responsible for the protection of personal information, etc.). Prior to requesting consent from an employee, employees in most EU countries must be apprised of their rights.

In **Canada**, the situation is similar to that of Europe – consent of employees is required prior to commencing monitoring of the workplace, and additional legal requirements apply to the processing of personal information. The Personal Information Protection and Electronic Documents Act defines these requirements.

Protection of personal information is now regulated in **India** as well. The protection is codified in an amendment known as The Information Technology Principles (or Privacy Principles), which is based on the European approach and imposes similar requirements and the employer.

The law systems of **Australia** and **New Zealand** are similar to each other as far as employee monitoring is concerned. A policy-driven approach is preferred in both countries. The systems support employers in the creation of internal policies that govern the enabling/disabling of informational sources in the company and clarify the possibility of monitoring, including its extent and other details concerning it.

The approach to employee monitoring is not unified in **Latin America**. Many countries have recently adopted the tenets of personal information protection from the European law. Mexico, for example, has sanctioned an act on the protection of personal information, which is based on a Spanish original. In some Latin American countries however, a position to monitoring is not embedded in the law, and companies follow common court decisions.

Differences exist in how consent to monitoring is granted. While in some countries, sufficiently informing the employees, i.e. via an internal Internet or e-mail use policy, is sufficient (e.g., Hong Kong, Japan, or the USA), direct and undisputable consent to monitoring in the workplace is required from individual employees elsewhere (e.g., South Korea, SAR, or Europe).

An up-to-date overview of recommendations on how to achieve compliance with regulations in individual countries when using Safetica can be found on the Safetica Technologies company website: www.safetica.com/safetica/regulatory-compliance.