MORRISON | FOERSTER

Legal Updates & News

Bulletins

Italy's DPA Publishes New Rules on Monitoring Employees

May 2007
by Karin Retzer, Teresa Basile

Privacy Bulletin, May 2007

PDF Version

On 10 March 2007, the Garante, Italy's data protection authority, issued a guidance paper which attempts to assist employers to overcome some of the hurdles and to allow monitoring in a way that satisfies the requirements of the EU[1] Directive[2] as implemented in Italy[3]. The paper contains a legally binding interpretation of the statutory requirements for monitoring in the workplace. Unfortunately, however, the paper resolves only some of the problems that global organisations are facing. It fails to address the question of whether fulfilling an extra-territorial legal obligation, such as responding to a discovery request under US rules, may legitimise monitoring.

The main provisions of the paper are highlighted below and show how employers can mitigate the risks.

The Requirements

Proportionality
As is to be expected, the paper rules out any systematic and constant monitoring through software or hardware devices to the extent it is aimed at "directly controlling" employees' activity. Information obtained through systematic monitoring is unlawful and cannot be used by the employer in court.

Compliance with Data Protection Principles
Any processing of personal data — including data obtained through internet or e-mail monitoring — must meet the requirements of Articles 6, 7 and 8 of the Directive:

First, employers may only monitor in compliance with the data protection principles. These principles are:

- Necessity: prior to monitoring, an employer must assess whether the monitoring in all its forms is absolutely necessary for the specified purpose. Less intrusive methods should therefore always be used if possible.
- Finality: data collected through the monitoring activity must respond to a specified, explicit purpose and cannot be processed for a different purpose.
- Transparency: the monitoring of activities must be transparent.
- Legitimacy: employers may monitor employees only to safeguard their legitimate interests and provided that they do not violate the employees' fundamental rights.
- Proportionality: personal data processed through monitoring must be adequate, relevant and not excessive with regard to the purpose for which they are processed. For instance, the monitoring of e-mails should focus on the traffic data of the participants and time of the communication rather than on the content of communications.
- Accuracy and retention of data: personal data captured through the monitoring activity must be updated and retained only for the period deemed necessary for the purpose to be achieved.
- Security: the employer must adopt all appropriate technical and organisational measures to ensure that any personal data are protected from alteration, unauthorised access and misuse.

In addition, monitoring is only permissible where there is a legitimate purpose.

The paper helpfully clarifies that monitoring for organisational, production or security reasons would meet those requirements. This means, for instance, that an employer can check his or her employees' professional emails during their absence if they are in charge of a project which must be finalised. Another example could be the necessity of implementing tools for the maintenance of the system, which indirectly can involve the monitoring of employees and consequently the processing of employees' data. In these instances, it is required that agreement with the Works Council is reached. Alternatively, authorisation must be obtained from the labour administration department.

The defence of a legal claim in Italian courts is also seen as serving legitimate purposes for monitoring and collecting personal information. No agreement with the Works Council is needed for such monitoring. One question the paper does not answer is whether employee records and communications can be monitored where international litigation is concerned. The generic reference to the "defence of a legal claim", without any specification of territoriality, could "potentially" be interpreted as embracing international litigation claims, but guidance by the DPA on similar conflicts of legal requirements suggests that only Italian litigation is contemplated. However, at the time of writing, Italy's DPA has not taken an official position on this point. In order to limit their exposure, it is therefore advisable for organisations to pre-screen documents to limit the collection and transfer of personal data and to adopt a best-practices approach, for example to ensure notice is provided and an acknowledgment of the employees in question obtained.

Notice

The paper specifies that employers must inform employees, including, at a minimum, the following:

1. the conditions for using internet and e-mail at work;
2. the extent to which private use of the internet and e-mail is accepted in the workplace;
3. the fact that e-mails may be monitored, and for what specific purposes;
4. what kind of information can be stored temporarily and who is authorised to have access to it;
5. the options to be agreed in case of an employee's absence;
6. the availability of private use of internet/e-mail subject to a charge being paid by the employee;
7. the security measures in place;
8. 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.

The information may, for example, be provided through a technology-use policy. In any event, covert monitoring is prohibited.

Security

Employers should also protect employees' rights by adopting certain technological measures to avoid opening employees' e-mails and to prevent the inspection of employees' web-surfing. A specific reference in this respect is made by the DPA to privacy enhancing technologies (PETs). Additionally, as a general measure, employers should collect data on an anonymous basis whenever possible. As for e-mail, employers should make available addresses to be shared by several employees (for example, info@ente.it). Also, employers should consider assigning two e-mail addresses (for corporate and private purposes). E-mail footers should be included in emails to warn recipients about the non-personal nature of the messages and possible access by the company to which the sender belongs pursuant to corporate policy. With respect to absent employees, the use of out-of-office replies with contact details for colleagues who should be contacted during absences should be encouraged, or employees should appoint a "delegate" entitled to check e-mails.

Data Retention

Employers should also develop data retention policies to ensure that employee data are deleted periodically and automatically (for example, by means of the log file rotation), unless needed for security or organisational reasons, defence of a legal claim, or request by a public authority.

Conclusion

While the paper largely rules out covert monitoring or monitoring indiscriminately, and thereby may require changes to practices, it is helpful in that it establishes that monitoring for security, production reasons or organisational purposes such as covering employees' absences or disciplining employees is permissible, provided employees are notified in advance and Works Council agreement has been obtained. Also, monitoring is allowed for the defence of a legal claim in Italian courts. As regards international litigation, employers are, however, largely left in legal uncertainty.

Employers retain and access employee communications and records for a variety of purposes, including preventing spam, protecting the IT infrastructure, intellectual property and other assets, and ensuring uninterrupted communications with customers and other business contacts during employees' leave of absence or after the termination of the employment relationship, etc. US discovery rules may also require employers to retain, search and produce records that may be relevant for pending or reasonably foreseeable litigation. For any records containing personal data from the EU1, employee monitoring may be at odds with privacy rights granted under EU data protection laws. Under the EU Data Protection Directive (95/46/EC) 2 any collection, use or transfer of personal data is restricted, covert monitoring is prohibited, and any data must be deleted as soon as the purposes for which they were originally collected have been fulfilled.

This article appeared in the May 2007 issue of Privacy Laws & Buisness *and is reprinted by permission.*
http://www.privacylaws.com/

Footnotes:

1: Any reference to the European Union (the "EU") should be understood as referring to the territory of the Member States. The 27 Member States currently are: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

2: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal information and on the free movement of such data ("Directive"), published in the Official Journal on 23 November 1995, L281/31, available at

http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46

3: *Provvedimento: Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori. (GU n. 58 del 10-3-2007)* Available in Italian at web page:

http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522

Dr Giovanni Buttarelli, Secretary General, The Garante (Italy's DPA), will speak on Italy's new employee monitoring rules, which he sees as setting the EU standard, at Privacy Laws & Business' 20th Annual International Conference at St John's College, Cambridge, UK, 2-4 July. See www.privacylaws.com/ac20