SUMMARY

2010/37: Personal data protection in employment (PL)

<p>The employment relationship does not guarantee that consent to process his or her personal data is given freely by the employee. The provisions of the Polish labour law provide an exhaustive list of data which an employer may demand. The use of biometric data to control working time is disproportionate to the objective which it seeks to attain.</p>

Summary

The employment relationship does not guarantee that consent to process his or her personal data is given freely by the employee. The provisions of the Polish labour law provide an exhaustive list of data which an employer may demand. The use of biometric data to control working time is disproportionate to the objective which it seeks to attain.

Facts

"L" is a Polish company belonging to an international corporation producing consumer electronics. L installed fingerprint reading devices to record working time at the entrance to its factory and offices. The use of the new system was entirely optional, since in parallel with the fingerprint readers there were also magnetic card readers. The employees could choose which device to use to record their working time.

The Polish Labour Code (the "Code") stipulates that "the employer shall have the right to demand from any person seeking employment the following personal data: (i) name(s) and surname, (ii) parents' names, (iii) date of birth, (iv) place of residence (address for correspondence),(v) education and (vi) employment record. In addition to the personal data referred to above, the employer shall have the right to demand that the employee provide: (i) other personal data of the employee, including names and surnames as well as dates of birth

of the employee's children, if this is required to enable the employee to benefit from special rights provided in the labour law; and (ii) the employee's PESEL number (Polish resident identification number). Matters which refer to the above data, beyond the scope of the Code shall be subject to the provisions of the Act on Personal Data Protection of 29 August 1997 (the "Act")."

Following Directive 95/46/EC1, the Act sets forth a number of conditions for legitimate processing of personal data including, in particular, the consent of the data subject or pursue of the legitimate interests by the controller or by the third party or parties to whom the data are disclosed.

Administrative procedure

In February 2008 the Inspector General for the Protection of Personal Data (Generalny Inspektor Ochrony Danych Osobowych) "GIODO", issued an administrative decision in which it obliged the company to erase personal data collected from employees in the form of fingerprint records and cease collecting such data. According to GIODO, the company, as a data controller, breached the provisions of the Act by processing data without legal grounds for doing so. In April 2008 GIODO upheld its decision.

Court proceedings

The regional administrative court (Wojewódzki Sąd Administracyjny, the "WSA") in Warsaw overturned GIODO's decision. The Court acknowledged that the processed fingerprints were the employees' personal data but pointed out that the data was obtained upon the employees' written consent, given for that particular purpose. As the Act specifies the consent of the data subject as grounds for personal data processing, the Court recognised that the company had acted in compliance with the law. As to the relationship between the Act and the Code, the WSA stated that processing of personal data other than data listed in the Code is possible based on the Act. The Act sets forth autonomous conditions for the processing of personal data including, in particular, the consent of the data subject, along with pursuit of legitimate purposes of data controllers or recipients.

GIODO filed an appeal on points of law against this judgement to the chief administrative court (Naczelny Sąd Administracyjny, the "NSA"). In the appeal it stated that only data enumerated in the Code could be collected. Collecting other personal data of employees by the employer would be considered as an intrusion into employees' privacy. What is more, employees would lack any real freedom to choose when consenting to the processing of their personal data because of the nature of the employment relationship.

Judgment

The NSA revoked the decision of the WSA. In brief justification, the NSA stated that on account of the lack of balance in employment relationships, employee consent may not constitute legal grounds for the processing of biometric data. It is for that reason that the legislator limited the scope of the data that employers may demand from employees. To allow employees' consent to legitimise the use of biometric data would circumvent the provisions of the Code.

Further, with regard to the adequacy principle set forth in the Act, consent may not be used to extend the scope of the personal data provided for in the Code. The adequacy principle provides that personal data must be adequate in relation to the purpose for which it is processed. The NSA referred to Article 29 of the Directive by which a consultation body was appointed to safeguard the homogeneous application of data protection in the EU. The NSA stated that it assessed the principles of legality and adequacy with relation to the question of biometrics. If the principle of adequacy is the main criterion for the assessment of the processing of biometric data, according to the NSA, using biometric data to control working time is disproportionate to the original purpose of data processing. Further, it shared the consultation body's view, as expressed in the working document of 1 August 2003, that in matters of employment and labour law, the consent of the employee may be referred to if the employee has freedom to give such consent and the right to refuse to do so without suffering harm.

Commentary

The interesting thing here is that the Polish administrative court pronounced itself not only on a very important labour law issue, but also incidentally gave its interpretation of European law. However, the rather short reasoning of the NSA is not convincing. On one hand the NSA refers to the need for freedom to consent in biometric matters but on the other, it fails to address the fact that in this particular case, freedom of choice was guaranteed by the retention of the "old fashioned" magnetic readers by the employer. Nor does the Court explain why the processing of fingerprints is not adequate for the purpose of controlling working time. One can only speculate as to whether the answer would have been different if security purposes had been raised by the employer. On the other hand, an interpretation of the Code given by the NSA and one which is shared by most commentators - deprives employees of rights which the Act confers on all subjects of the law. In other words, the fact that they are employees prevents them from giving consent in those areas where other people - not employees - could give consent. Far from depriving people of rights granted by other provisions of law, labour law aims to protect the weaker party in the employment relationship, and for this reason one

might question the validity of the NSA's conclusions.

Academic Comments

Poland (Prof dr hab. Andrzej M. Świątkowski): After a period of over half a century since WWII of extensive control of citizens by the state, Poles are nowadays very sensitive when it comes to issues of privacy.

There is a question as to whether legal guarantees in the context of the relationship between citizens and the state may be applied to the employment relationship. After all, the Code makes provision for freedom of choice to be enjoyed by each individual able and ready to work when it comes to entering into employment relationships. That most characteristic feature of the employment relationship is the principle of equality of parties, applied as between the employer and employee. According to the NSA in Warsaw, the Code does not take into account this idea of equality and prohibits all employers from demanding any additional personal information from their employees.

I personally do not share the view that the Polish legislator seeks to limit the scope of personal data which the employer may receive from his or her employees. There is no legal basis for the assertion that the parties to an employment contract may not voluntarily agree that the employee will provide additional information sought by an employer who finds it necessary. I

n the case presented by Dr Marek Wandzel, the EELC national correspondent for Poland, the scope of any additional information was not addressed directly by the NSA. However, it is common knowledge that biometric data may serve different purposes. In the case at hand, it was used only as evidence that employees reported to work on time. Thus, in relation to the problem of data protection at issue in this case, it is necessary to state that the employer may not demand to have data that is not listed in the Code from an employee but this legal obstacle cannot be extended to those cases in which an employee volunteered to provide such data.

In the current case it was not established that biometric data may serve malicious purposes and there was no evidence supporting the proposition that the employer must be treated as not acting in good faith when using modern technical devices to keep records about his employees in matters directly related to adherence to working time rules.

Comments from other jurisdictions

The Netherlands (Catherina Jakimowicz and Marta Borrat I Frigola): The general boundaries for Dutch employers when processing personal data of employees in the context of an employment relationship are found in the Dutch Data Protection Act (DDPA).

According to the DDPA, one of the legal grounds permitting data controllers to process personal data is the unambiguous consent of data subjects. The key issue when analysing the facts of this particular case in the light of Dutch law is whether consent has been unambiguously provided. According to the Explanatory Note to the DDPA (Explanatory Note), unambiguous consent is subject to strict requirements. It means that consent: a) is freely provided, b) is provided in relation to specific data processing and not generally, and c) should be ÒinformedÓ, i.e. the data subject should know what he or she is consenting to.

This first requirement can also be found in the opinion of the Article 29 Working Party. According to this opinion, the specific hierarchical relationship between employer and employee implies that employee consent cannot be freely given and, therefore, may be considered void. Even so, the Article 29 Working Party seems to slightly nuance its opinion and seems ready to accept employee consent if the employee has had a genuinely free choice and is able subsequently to withdraw such consent without detriment.

These rather strict views on "free consent" do not sit well with the daily practice of employment law. There are many situations conceivable where the employee is asked for his consent. Take for example a non-competition clause agreed upon prior to or during the employment contract, which may have severe consequences for the employee. The validity of such consent, once given, is normally not doubted.

From a Dutch perspective it is noteworthy that the Polish NSA seems to omit that employees in this specific case had a genuinely free choice: the old system of time registration through magnetic card readers existed alongside the biometrical registration system. Employees refusing to opt for the biometrical system would still have had the option of time registration by other means. We do not know whether refusal to agree to the biometrical registration system would have resulted in detrimental consequences for the employees involved. However, assuming that this is not the case, and since a genuine choice existed, a Dutch court would have had reason to decide that consent was valid grounds for the processing.

Nevertheless, for another reason, the Dutch courts could still have decided that the use of biometric registration methods violates privacy laws and that is the principle of proportionality and adequacy. Legal literature recognises the advantages of using biometrics, but it also highlights that such methods are not free of risk. If a biometric character, such a fingerprint, is compromised the data subject may suffer negative consequences (for example if this data is abused) and it may take a very long before the error or abuse is repaired. Biometrics should be applied taking into account, among other things, the most reliable techniques in order to preserve the data from illegitimate use or loss. In addition, and as an expression of the principle of proportionality, the use of biometrics should be limited to those

cases where it is strictly necessary and where less severe measures do not serve the specific purpose for which biometric registration would be required. Since a working alternative is available for the employer (the magnetic card readers) which has less impact on the privacy of the employees, a Dutch Court might rule that the decision by the employer to use the biometric registration system is not in line with the Dutch Data Protection Act, as it violates the principle of proportionality and adequacy.

Germany (Silvia C Bauer): The legal boundaries of processing personal data of employees are mainly governed by the Federal Data Protection Act (BDSG).

Usually, any collection, processing or use of personal data is lawful provided that a statutory legal basis is available or the employee has given his or her explicit consent (section 4 of the BDSG).

The statutory legal bases for collection, processing and use of employees' personal data are to be found, for example, in section 32 BDSG, which was introduced as a new provision of the reformed BDSG in September 2009 and explicitly regulates the handling of employees' data. By section 32(1) of the BDSG employees' personal data may only be collected, processed or used for employment-related purposes if this is necessary to enable a decision on whether to establish an employment relationship to be made or, after it has commenced, for its execution or termination, including all collection and processing of personal data which is necessary for the performance of the employment contract, e.g. the transfer of data to payroll providers.

However, if special categories of data, such as health data or data related to race are processed, this cannot be justified under section 32 of the BDSG because processing of these kinds of data is always considered to be an intrusion into the employeeÕs privacy. Only in quite exceptional cases would this be acceptable (as regulated in section 28(6) of the BDSG). Otherwise, the freely-given consent of the employee must be obtained.

There is no doubt that the processing of biometric data involves an intrusion into employee privacy. The storage of biometric data may be very problematic if the data includes, for example, information about the race or state of health of the employee. Moreover, according to section 4a(3) of the BDSG, the employer must obtain the explicit consent of employees in case sensitive data about them are collected, processed or used. By section 4a of the BDSG the consent must fulfil the following requirements: (1) it must be in written form, (2) freely provided, (3) given for defined purposes (4) and the employee must have been informed of the consequences of refusing to consent. If in the circumstances the employee is not likely to know to whom the data may be disclosed, he or she should be informed, at the time of giving consent, of the categories of recipients.

It is greatly disputed in Germany as to whether an employee can give his or her consent freely. Some data protection authorities in Germany (the competent authority differs according to the registered office of the company) have ruled that in employment relationships, consent may not be obtained freely - and therefore not validly - as employees may be under pressure to give their consent. At the time of writing, this view has not been expressed as a general view or ruling of the data protection authorities so that consent may be assumed to be available as an alternative approach. However, in each case the consent will be considered unlawful if refusal to it would result in detrimental consequences for the employees involved.

The principles of "data avoidance" and "data minimisation" (stipulated in section 3a of the BDSG) as well as of proportionality and adequacy, must be borne in mind while processing data in a biometric registration system. For example, the employer must ensure that adequate technical and organisational measures are taken to protect the data, that special categories of personal data (such as fingerprints) are processed separately from other personal data collected from the employee and that only necessary data is processed. Processing of this kind may involve high risks that the privacy of the employee could be abused, which must be weighed against the interests of the employer in using the system.

There is a particular restriction relating to the supervision of employees by an employer under the Works Constitution Act. According to Section 87 I nos 1 and 6, if technical equipment to be used to supervise the behaviour or performance of employees is to be introduced, it is necessary to obtain the consent of the works council. Hence the use of a fingerprint device for recording working time would, under German law, need the consent of the works council.

Czech Republic (Natasa Randlova): According to the Czech Labour Code, an employer may not give notice to its employee during a protective period, for example during a female employeeÕs pregnancy. The Czech Labour Code further specifies some exceptions to this rule (e.g. in case of the employer closing). Moreover this rule does not apply to terminations of employment during a probationary period or terminations of employment by agreement. At the same time the Czech Labour Code explicitly forbids employers from requiring employees to disclose pregnancy or from obtaining this information through third parties. Despite this, the Czech court would decide in the same way as the Hungarian Supreme Court, i.e. that the dismissal during an employee«s pregnancy is unlawful even if the employee had not previously informed the employer of her pregnancy and even if the employee was unaware of her pregnancy. Already in 1966 the Regional Court decided that terminating employment while a female employee is pregnant is not valid even though the employer was unaware of this pregnancy.

Footnote

1 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 data and on the free movement of such data.

Subject: Privacy

Parties: L - v - Inspector General for the Protection of Personal Data (GIODO - Generalny Inspektor Ochrony Danych Osobowych)

Court: Chief Administrative Court (NSA Naczelny Sąd Administracyjny)

Date: 1 December 2009

Case number: I OSK 249/09

Hard copy publication: -

Internet publication: http://orzeczenia.nsa.gov.pl

Creator:
Verdict at: 2009-12-01
Case number: I OSK 249/09