BNA

Privacy & Security Law Report

How to Monitor Workplace E-Mail and Internet in Europe: The Polish Perspective

BY KARIN RETZER AND JOANNA LOPATOWSKA

In many countries, employee monitoring is an everyday reality. The most common form of monitoring is e-mail and internet use monitoring.[1] As with many European laws, Polish law does not provide specific rules for the monitoring of workplace communication such as e-mail, telephone, or internet use, or monitoring via video surveillance or geolocation. Polish courts have not dealt with the question in detail, and there is no specific guidance from the Inspector General for the Protection of Personal Data ("GIODO"). Rather, monitoring is subject to general labor and data protection rules, which makes compliance challenging. Below we describe the key approaches to monitoring across Europe and in Poland, and recommend how organizations with personnel in Poland might comply with local laws.

EUROPE

The key European Union/European Economic Area [2] data protection legislation—the 1995 Data Protection Directive[3]—does not deal with any specific aspect of employment relationships. It neither provides rules on employee monitoring, nor on monitoring in general. Instead, it sets out general provisions on the collection and processing of personal data. These provisions are then further interpreted by individual Member States who implement them in their national legislation. In the wake of a series of unsuccessful attempts to introduce EU/EEA legislation on the issue, there is little chance

[1] According to the 2004 Hitachi Data Systems' survey, on average in the EMEA [Europe, Middle East and Africa] region, 56 percent of employers monitor e-mail and 36 percent of employers monitor internet use.

Karin Retzer is of counsel to Morrison & Foerster, Brussels, where her practice focuses on electronic commerce and data protection, technology licensing, and intellectual property law. Joanna Lopatowska is an associate in the Privacy and Data Security Group in Morrison & Foerster's Brussels office.

[2] The 27 Member States of the European Union (EU) 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 (collectively, the "Member States"). Note that both the Data Protection Directive and the ePrivacy Directive apply to all EEA countries, *i.e.*, the EU Member States plus Iceland, Liechtenstein, and Norway.

[3] Directive 95/46/EC of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on free movement of such data [1995] OJ L 281/31.

 ISSN 1538-3423

that the European Commission will introduce specific rules on employee monitoring in its revision of its general data protection framework.

The Article 29 Working Party's Position

Due to its complexities and prevalence, the issue of employee monitoring has been extensively discussed at the EU/EEA level over the past decade. The Article 29 Working Party (''WP29''), a network composed of the Member State data protection authorities,[4] issued an opinion on the processing of personal data in the employment context in 2001.[5] The WP29 observed that monitoring of e-mails and internet access involves processing of personal data and thus falls under the scope of the EU Data Protection Directive and related Member State implementing legislation. According to the WP29, monitoring must be proportionate, not excessive for the intended purposes, and carried out in the least intrusive way possible.

The Opinion was followed by a 2002 Working Document[6] that examined the acceptable limits to monitoring electronic communications in the workplace. This Working Document emphasized that employees' rights to privacy in the workplace must be balanced with the legitimate rights and interests of the employer, such as business efficiency or the right to protect the employer from harm caused by employees' actions. In other words, the reasons for the data processing involved in monitoring have to be adequate and relevant, and data cannot be processed for any other purposes. The Working Document also specified that no sensitive data should be processed.

The WP29 generally recommends that monitoring should be avoided unless there is a specific and important business need. It suggests that before implementing monitoring policies, employers should consider whether monitoring is necessary and proportionate, and whether the same results could be obtained through traditional methods of supervision. In addition, the WP29 insists that monitoring must be transparent and that the processing of personal data be fair. Therefore, prior notice informing employees about monitoring is essential. Notice may be delivered by software such as a pop-up warning window alerting employees that the system has detected or prevented unauthorized use of networks.

The WP29 issued another Opinion in 2006 about the technology used for monitoring purposes.[7] This Opinion concluded that all online communications in the workplace are subject to confidentiality protection, including those sent from workplace equipment for private as well as professional purposes. The WP29 condemned many commonly used filtering and tracking technologies, even if used only for anti-virus and scan filtering, since any access to e-mail content, scanning, tracking, screening, interception, opening, and/or reading of communications might lead to a violation of an employee's right to privacy. The WP29 stressed the importance of providing employees with prior notice of monitoring, but failed to address how it should be delivered in practice in an online environment.

Although not legally binding, the WP29's opinions provide important guidance, and national data protection authorities take them into account when applying and enforcing national laws. For countries like Poland, where there are no laws or guidance on e-mail monitoring, the opinions are particularly useful sources of advice.

The EU/EEA Member States' Approach

Unlike Poland, some Member States have legislation or data protection authority guidance that specifically covers employee monitoring. However, views on the permissible scope of monitoring vary. Below we provide a brief overview of these approaches in key Member States.

- **France** has yet to enact specific legislation on employee monitoring but the general labor, civil, criminal, and data protection laws[8] apply. Also the CNIL, France's data protection authority, published guidance guidance[9] in 2005 that discussed practical issues related to the monitoring of employees' activities in the workplace. Before implementing monitoring, the employer must consult the employees' representatives. Importantly, any monitoring is subject to rules defined in technology use policies that form part of the internal rules within organizations. Intercepting employee telephone calls is prohibited by the French Criminal Code and is punishable by a fine and imprisonment up to one year. The approach to monitoring e-mails is different. In general such monitoring is permissible but its scope and duration must be reasonable. The employer must provide notice explaining the conditions under which it may intercept the messages. The employer must also establish a legal basis for the monitoring and obtain consent if required in specific circumstances. The CNIL recommends that particular caution be exercised with respect to e-mails marked ''private'' or ''personal.'' However, more recent jurisprudence seems to indicate the adoption of a less severe approach which allows employers to open files tagged as ''personal'' in the presence of employees.[10] French courts have also ruled or upheld rulings in favor of employers in cases where employ-

[4] The Article 29 Working Party is an advisory body on data protection and privacy. It was set up under Article 29 of Directive 95/46/EC of 27 October 1995 on the protection of personal data and the free movement of such data.

[5] Opinion No 8/2001 of Sept. 13, 2001 on the processing of personal data in the employment context, is available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf.

[6] Working document No 55 of May 29, 2002 on the surveillance of electronic communications in the workplace, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf.

[7] Opinion No 2/2006 on privacy issues related to the provision of e-mail screening services, WP 118, is available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_en.pdf.

[8] Act 1978 no. 17 of January 6, 1978, on Data Processing, Data Files and Individual Liberties.

[9] *Guidance is available at* http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf

[10] Cour de Cassation, Chambre sociale, Pourvoi no. 03-40.017. The Court stated that ''save in case of a particular risk or circumstance—and the possession of pornographic photos by the employee was considered not to fall inside any of the mentioned categories—the employer cannot open the folders identified by the employee as personal on his hard drive of the computer put at his disposal except if the employee is present.''

  PVLR ISSN 1538-3423

ees were dismissed because their employers discovered discrediting facts as a result of internet and e-mail monitoring.[11]

- **Finland** is among those countries that have enacted specific laws on the protection of privacy at work supplementing general data protection laws. The Act on Data Protection in Working Life,[12] places strict conditions on monitoring e-mail accounts assigned to an individual employee by the employer for work purposes. Thus e-mail messages may be monitored or opened only if, based on other evidence, the employee's inbox can be expected to contain messages to which the employer needs access, for business purposes, during an employee's absence. Further such access is only permitted if the employer has offered at least one of the following technical options to the employee: (1) through use of an auto-reply facility the employee can notify senders about his or her absence and about the person in charge of ongoing matters during the absence; (2) the employee can forward messages either to another employee or to an acceptable external e-mail account; or (3) the employee can consent to another employee receiving his e-mail messages for the purpose of ascertaining whether there are messages that are necessary for the employer's business. In practice this means that without the employee's consent, the employer may never use administrator rights to access employee e-mails for disciplinary purposes, or while the employee is present at work or otherwise available to review his/her e-mails. It is doubtful whether the employee can even effectively consent to such access. The Finnish Act also provides detailed conditions on the process of opening and reporting on the opening of messages and of dealing with messages in situations where the nature of the message is not apparent, for example, if an employee works independently and the employer has no system in place to account for matters handled by that employee. Before implementing monitoring, the employer must notify the employees about its purposes, the timeframe for the implementation, and the methods of monitoring used. Implementing monitoring schemes must be also discussed in consultation with the employee representatives.[13]
- In **Germany** the legal situation is rather ambiguous. Currently, where use of work equipment for private purposes is permitted or tolerated, the employer acts as a ''telecommunications services provider'' for employees and is thus subject to telecommunications secrecy rules and regulations. According to these rules,[14] employers may not access private e-mails, nor any work related e-mails, unless private and work related e-mails can be clearly separated, *e.g.*, through separate e-mail accounts. This interpretation has been confirmed by a November 2010 judgment of the Bonn District Court[15] which determined the criminal liability of a manager who monitored the telephone calls of employees suspected of leaking confidential company information to the press. A government-approved draft bill on employee privacy is under discussion in the Federal Parliament which would amend the country's framework data protection law.[16] This bill would permit limited monitoring only to facilitate the enforcement of policies that prohibit personal use. However, it fails to address personal/private use of telecommunication systems where such use is permitted. Since the bill rules out consent, it will no longer be possible to permit personal use of such systems in exchange for the employee consenting to some limited monitoring, so organizations operating in Germany would be well advised to prohibit any personal use of telecommunications systems.
- In **Spain**, Article 20(3) of the Workers' Statute[17] provides that an employer is entitled to verify the fulfillment of an employee's work obligations. However, this right must be balanced with the fundamental privacy rights and right to secrecy of communications respectively of Sept. 26, 2007[18] (confirmed by another recent judgment[19] of March 8, 2011), the Supreme Court ruled that, for this balance to be met, at least (i) prior and comprehensive information on the relevant monitoring actions must have been provided to employees and (ii) the employer must prove that the specific monitoring action is proportionate. The Spanish DPA has followed the main lines of this judgment regarding legitimate data protection grounds: it has considered that compliance with article 20,3 of the Workers' Statute, as construed by this judgment, is the legitimate ground for an employer to process the personal data of employees that results from monitoring actions in the workplace. However, from a criminal point of view, it is not that clear whether the above requirements would be deemed sufficient in all situations (the general rule being the consent or a court authorization).
- In the **United Kingdom**, in 2005 the Information Commissioner's Office (''ICO'') issued an Employment Practices Code[20] that focused on monitoring in detail. Under the Code, before implementing

[11] See recent rulings of the Cour de Cassation of March 4, 2011, docket number unavailable, opinion released 3/4/2011; of December 15, 2010.

[12] The Act on Data Protection in Working Life, Laki Yksityisyyden Suojasta Työelämässä, 13.8.2004/759.

[13] In accordance with the Act on Cooperation Within Companies: Laki yhteistoiminnasta yrityksissä 22.9.1978/725.

[14] *See* Telecommunication Act available (in German) at http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf

[15] *See* LG Bonn Az 23 KLs 1010, available (in German) at http://www.telemedicus.info/urteile/Telekommunikationsrecht/1283-LG-Bonn-Az-23-KLs-1010-Spitzelaffaere.html

[16] The amendments are not yet in force—they are still waiting to be passed by Parliament.

[17] *See* http://noticias.juridicas.com/base_datos/Laboral/rdleg1-1995.html

[18] Judgment of Sept. 26, 2007; see also judgment of Nov. 6, 2008 of the High Court of Justice of Galicia; judgment of Sept. 16, 2009 of the High Court of Justice of Madrid.

[19] *See* http://portaljuridico.lexnova.es/jurisprudencia/juridico/61380/sentencia-ts-sala-4-de-8-de-marzo-de-2011-uso-en-el-trabajo-de-medios-informaticos-vigilancia

[20] The Information Commissioner's Office published the Employment Practices Data Protection Code on June 14, 2005. The Code is available at http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/

any monitoring, employers must conduct an impact assessment that: (i) identifies the purposes of the monitoring and the benefits it is likely to deliver; (ii) identifies any likely negative impact of the monitoring scheme; (iii) considers alternatives to monitoring or the different ways in which it may be carried out; (iv) takes into account the obligations that arise from monitoring; and (v) assesses whether the monitoring is justified. In addition to the Code, the European Court of Human Rights addressed the rules on employee communications monitoring in the United Kingdom. In a landmark ruling concerning the monitoring of an employee's telephone calls without her knowledge, the European Court of Human Rights[21] found that the employee's privacy was breached because monitoring of telephone calls and e-mail was implemented without the employee's knowledge. The Court acknowledged that for monitoring to be lawful, employees must be provided with prior information about the monitoring and its purposes.

POLAND

Current Legal Framework

In the Polish legal system there is neither relevant legislation nor GIODO guidance that expressly permits employee monitoring or defines its permissible scope. Furthermore, it is unlikely that any such legislation will be put forward in the near future. According to the Minister of Labor and Social Policy, who would be responsible for proposing new legislation, the current labor law[22] provides sufficient grounds to assume that employee monitoring is legitimate.[23] E-mail monitoring is therefore permitted within the limits of the following general principles:

- First, to safeguard their interests, employers must be able to verify the work outcomes and the efficiency of their employees. To that end the Labor Code imposes on the employer the duty to organize working time effectively. (Article 94(2). This gives the employer the right to verify work product and indirectly permits employee monitoring.
- Second, employees have a reasonable expectation that they benefit from a degree of privacy in the workplace, extending to e-mail and internet use.[24] In this respect the Labor Code obliges the employer to respect the dignity and other personal interests of employees (Article $11^{(1)}$). The Polish Civil Code protects privacy of communications as a personal interest, *i.e.*, a personal right, subject to a general civil law protection (Article 23). In addition, the Polish Constitution enshrines privacy of communications as a fundamental right (Article 49).

Secondary legislation contains more concrete provisions. Based on the Labor Code, the Minister of Labor and Social Policy issued a regulation[25] that applies to all forms of work where computers are used and prohibits using quality control mechanisms on employee work product if these are implemented without the employees' knowledge. This means that e-mail monitoring is legitimate if notice is provided.[26] Unfortunately, this provision is ambiguous and it does not explain exactly what ''quality control'' is, or whether installing monitoring software is permitted.

Collection of employee data

E-mail monitoring involves the processing of personal data. The Polish Data Protection Act[27] only provides general rules applicable to any data processing. Therefore, the Labor Code must be considered. Unfortunately, the Labor Code only allows for the collection of very limited and expressly listed data (Article $22^{(1)}$), and this does not correspond with common practice in many organizations.[28] Only a basic set of data is covered, including name, parents' first names, date of birth, address, educational background and work history, national identification number, and some other data which are limited in scope.

Article $22^{(1)}$ is therefore strongly criticized for imposing unreasonable limits on the collection of employee data. The GIODO recognizes these limits but emphasizes that the failure to reflect the business realities in the Labor Code does not *per se* legitimize violations of the Data Protection Act.[29] This rather narrow interpretation is not reflected in practice by the GIODO so enforcement of Article $22^{(1)}$ remains weak.

Through monitoring, employers may potentially obtain unlimited amounts of information about employees, and this may lead to violations of Article $22^{(1)}$. Although some commentators have argued that the Labor Code does not exclude the voluntary disclosure of other data by employees, the Polish Supreme Administrative Court (''NSA'')[30] does not agree. In a case concerning the collection of employees' biometric data to verify their working time, the NSA stated that such measures are disproportionate and that other means are available to achieve this purpose. Furthermore, the NSA underlined that consent in this respect is not a sufficient legal

documents/library/Data_Protection/Detailed_specialist_guides/EMPLOYMENT_PRACTICES_CODE.ashx.

[21] Judgment of April 3, 2007, Application No 62617/00. See also judgment of July 3, 1997, Application No 20605/92.

[22] *See* http://isap.sejm.gov.pl/DetailsServlet?id=WDU19740240141

[23] On Dec. 20, 2007 the Ombudsman addressed the Minister of Labor and Social Policy with a request to propose legislation concerning the controlling powers of the employer (RPO-561580-III/07/MRP). This, however, did not result in any legislative proposal.

[24] See judgment of the European Court of Human Rights of April 3, 2007, Application No 62617/00 ; judgment of Nov. 23, 1992, Series A No. 251/B, para. 29.

[25] Regulation of the Minister of Labor and Social Policy of December 1, 1998 on safety at computerized workplaces, Official Journal of December 10, 1998, No. 148, Item 973.

[26] Point 10 letter e of the Annex states the following: ''*while designing, selecting and modernizing the software and planning the carrying out of activities with the use of the monitor screen the employer must not perform the quantitative and qualitative control without the knowledge of the employee*''.

[27] Act on data protection of Aug. 29, 1997, Official Journal of 2002, No 101, Item 926, most recent amendment Official Journal of March 7, 2011, No 229, Item 1497 (ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych). The Act is available at http://isap.sejm.gov.pl/DetailsServlet?id=WDU19971330883

[28] See also GIODO explanations: http://www.giodo.gov.pl/348/id_art/971/j/pl/.

[29] See GIODO Decision No DIS/DEC-Dot. DIS-K-421/141/09.

[30] Judgment of Dec. 1, 2009, I OSK 249/09.

  PVLR ISSN 1538-3423

basis for data processing. In practice, the implications of this judgment not only concern biometric data; the judgment also limits the use of consent as a legal basis for employee data processing. However, as the NSA indicated, it is crucial to establish whether the collection of certain employee data is adequate and proportional for its purpose. If it is, monitoring of performance of work duties is permitted, provided the monitoring itself is adequate and proportional. Permanent monitoring of all employees' activities without clearly defined purposes would be unlawful.

Existing practice: Requirements for employee monitoring

Both the Minister of Labor and Social Policy and the GIODO agree that employee e-mail monitoring may be necessary to ensure the proper functioning of an organization. This is legitimate because employers own the devices the employees use, and are responsible for organizing the work of their employees. Employees, on the other hand, must use their working hours effectively.

According to a letter from the Minister of Labor and Social Policy,[31] employers may monitor the professional e-mail account of an employee. They may also read an employee's professional communications and grant other employees access to professional communications. The GIODO also accepts that employers may monitor employees' professional communications, including professional e-mail, hard drives, software, etc. Thus, in practice, employers have rather broad opportunities to monitor employee e-mails and internet use, provided:

- monitoring is limited to supervising work activities;
- monitoring is adequate for its purpose and does not violate the dignity and/or other personal interests of the employees; and
- employees are informed before the system is implemented.

However, employers must not monitor private communications. First, such monitoring would directly violate employees' right to privacy and secrecy of communications. Second, even if employees expressly consented to such monitoring, their consent would not be sufficient because the courts and GIODO contest consent in the employment context.

Obligation to provide notice, no consent requirement

Employees must be aware of any monitoring. Thus, GIODO emphasizes that the employees must receive specific and up-to-date information before monitoring systems are implemented. However, there is neither law nor GIODO guidance that would require notice to be delivered every time e-mails are monitored. In contrast, it is up to the employer to decide on the method of providing notice. Therefore, a blanket notice would be sufficient and an employer has several options:

- include the notice in the employment contract;
- include the notice in the internal work regulations communicated to all employees, which is the most commonly used method;[32] or
- provide a self-standing notice, either on paper, via e-mail, or via software such as a warning pop-up window.

Article 24 of the Polish Data Protection Act mirrors Article 10 of the EU Data Protection Directive 95/46/EC, in that it lists the same minimum notice requirements: information about the identity of the data controller, purposes of data collection, the data recipients, and the right to access and rectify data. Therefore, as monitoring serves specific purposes, the notice should at least describe:

- the purpose of the monitoring and how information collected in the process will be used;
- how or when information is collected; and
- to whom the information will be disclosed.

Whether express employee consent for e-mail monitoring is necessary remains disputable. However, such requirement appears to contradict both the GIODO and the Supreme Administrative Court's position on the validity of employee consent. In addition, the regulation regulation[33] on safety in computerized workplaces only requires notice. Therefore, notice seems sufficient. This is the current approach of the GIODO.[34]

Registration obligations

The Polish Data Protection Act provides for a broad and general exemption from registration of employee data. However, if data are transferred outside the EEA to a country that does not guarantee an adequate level of data protection,[35] one of two approaches may be pursued: employee consent or GIODO authorization.

- In the first case, an employee's explicit and written consent to the transfer removes the necessity for authorization by the GIODO.
- In the second case, employee consent is no longer required. Importantly, GIODO authorization also covers future employees. The procedure is free of charge and involves filing an authorization request, which is usually followed by questions from the GIODO. If the employer relies on the European Commission's Standard Contractual Clauses, ad hoc contracts, or Binding Corporate Rules for data transfer, a copy of the safeguards translated into Polish must be filed together with the authorization request. The procedure usually takes two to five months.

Transfer of employee data outside the EEA to countries that are considered ''adequate'' may begin after it has been authorized by the GIODO, or employees have consented in writing. Transfers to ''adequate'' countries do not require GIODO authorization, employee consent, or any other form of registration.

[31] Letter of Jan. 24, 2008 to the Ombudsman of DPR-I-0712-6/JS/MF/07, available at http://www.rpo.gov.pl/pliki/1201784465.pdf.

[32] In Poland, an employer is obliged to implement work regulations if it has more than 20 employees. If it has fewer than 20 employees, other methods of work organization may be considered.

[33] *See* http://pip.gov.pl/html/pl/doc/pdf/027.pdf.

[34] See interview with GIODO of March 1, 2011 at http://www.giodo.gov.pl/393/id_art/3970/j/pl/.

[35] As determined by the European Commission, adequate countries currently are: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Switzerland, and the U.S. Safe Harbor Framework.

Risks of non-compliance

If employers fail to apply the rules on monitoring and do not provide prior information to employees, they risk legal action and sanctions. The violation of the privacy of communications is a violation of personal interests. Therefore, an employee may file a civil damage lawsuit. Unauthorized access to other people's correspondence is also a criminal offense. Polish Criminal Code penalties include a fine of up to approximately €250,000 (approximately $360,000), or imprisonment for up to two years. However, enforcement of these provisions has, until now, been very limited. In addition, an entity that implements an excessive monitoring policy may be subject to inspection and audit proceedings by the GIODO, and may also be subject to that authority's subsequent decisions, which could include sanctions such as remedying the negligence; completing, updating, correcting, disclosing, or not disclosing personal data; or erasing the personal data.

How to ensure compliance in Poland

Taking into account the existing legal framework and practice, and the EU context, employers operating in Poland may consider the following steps to ensure lawful implementation of e-mail and internet monitoring systems:

- Consider whether monitoring is necessary and proportionate or whether the same results could be obtained through traditional methods of supervision.
- Clearly set out the rules on the use of work computers and software for private purposes. Inform employees about whether the private use of e-mail and the internet is permitted, and about the conditions and limitations of such use. Explain the consequences of unauthorized private use.
- Explain whether employees may use work e-mail for private correspondence, or whether the use of a private e-mail account is required for this. Consider providing employees with two e-mail accounts, one for professional purposes, monitoring of which would be possible, and one for purely private purposes, which would not be monitored.
- Provide notice to inform employees that their professional communications will be monitored. Explain the purpose of the monitoring, how employee data is collected, and to whom it is disclosed. The description should be clear and comprehensive. In particular, clarify whether the monitoring relates to all employees or only to selected sections of the organization and what use, if any, will be made of data collected through monitoring.
- Consider the most effective method of delivering the notice: through the employment contract, in the internal work regulations, or as a self-standing notice.
- Clarify that the use of work e-mail for private correspondence might result in unintended access if private correspondence is not clearly distinguished.
- In case of doubt as to whether communication is of a private or professional nature, ensure that employees have priority to access such correspondence. Otherwise, employers may risk accusations of violating privacy.
- Seek employee consent or GIODO authorization if data obtained through monitoring is to be transferred to affiliates or a parent company located outside the EEA in a country that is not deemed adequate.

  PVLR ISSN 1538-3423