Newsletter - TerraLex Connections

Particular Aspects of Personal Data Processing Activities in Day to Day Activity of a Romanian Company

By Iulian Popescu*

1. Introduction

Nowadays, when technology has become omnipresent in the everyday life of both individuals and legal persons worldwide, where a great number of personal data is revealed in view of performing routine activities and where the cyber security breaches have become more and more frequent, even at the highest level of a society, personal data flow particularities and the protection of such data against unlawful access has become a fervent concern of both public and private entities worldwide.

2. General aspects regarding personal data protection in Romania

In Romania, with few exceptions, personal data processing activities can be legally performed only after a prior notification is submitted to the National Supervisory Authority for Personal Data Processing ("**Data Protection Authority**") by the data controller. The obligation to notify the aforementioned authority devolves upon any data controller established in Romania or established abroad, but which processes personal information through any means located within the Romanian territory [1]. Hence, considering the aforementioned rules, a wide range of daily personal data processing activities performed by Romanian public or private entities or by multinational companies that also provide services in Romania are under the incidence of the notification obligation.

As regards the multinational companies having a local presence in Romania and which process personal information by using means located on the Romanian territory, there have been a series of discussions on which entity (*i.e.* the parent company or the local branch) should submit the notification to the Data Protection Authority, as a data controller. The applicable law provides that a foreign entity processing personal data locally must appoint a representative located in Romania [2] for the purpose of fulfilling the legal requirements with respect to the notification obligation. This approach would entail that the parent company, which is headquartered abroad, will act as a data controller and its Romanian branch will be its representative in Romania, in accordance with the law.

Apart from the regular analysis to determine which entity is the actual data controller, a continuous flow consultation with the Data Protection Authority is also advisable in order to determine the best hassle free approach, depending on the categories of data processed and the scope of such processing. We emphasize on this approach, as it ensures a better protection of data subject's rights and also helps establishing a better contact between the Data Protection Authority and the data controller, with regard to any possible issues that may occur with respect to the personal data processing activities.

As regards the notification process, mention should be made that this tends to get extremely complex and implies significant time resources. The first step of the process, which consists of delimiting each data processing activity and assigning it to a specific purpose, requires an in-depth analysis of all the activities performed by a certain data controller. In this respect it is worth mentioning that the data protection applicable legislation provides that each processing purpose must be notified separately, except for those purposes which can be correlated with each other. *Correlated purposes* are those similar in scope and those amongst which there is a connection that permits the data controller to provide them to the Data Protection Authority within the same notification form (*e.g.* purposes such as marketing and organizing contests for publicity purposes). In addition, data controller must also consider the requirement to clearly and specifically provide within the notification all the categories of processed personal data and processing purposes. Processing of a different category of personal data which has not been mentioned within the notification form shall be considered illegal if performed outside the scope and shall engage data controller's liability, in accordance with the law.

Moreover, there might also be cases where different entities are performing a series of activities implying personal data processing, but without being aware of the necessity to submit a notification regarding such activities. One of the best examples in this regard revolves around the widely spread practice of companies towards monitoring and protecting their premises by means of CCTV systems. This practice requires a separate notification to be submitted, with the observance of both primary and secondary legislation issued by the Data Protection Authority.

Also, there are certain situations when companies consider that the activities they perform are exempted from the obligation to submit a notification, but they are not aware of certain specific aspects which set aside the applicability of such exemption. For instance, processing personal information by the competent departments or persons within the entity, for the purpose of performing day-to-day human resources administration or financial-economic and administrative management does not generally trigger the necessity of a notification. However, this exemption shall not apply if the collected data is transferred abroad.

It is also noteworthy to mention that transfers abroad of personal information also requires the observance of a distinct set of rules and conditions expressly provided by the law. As such, personal information may be transferred abroad only if (i) *the provisions of the Romanian law are not breached* and if (ii) *the state to which personal data is transferred ensures an adequate level of protection of the personal data* [3]. Furthermore, such transfer is always subject to prior notification to the Data Protection Authority.

3. Particular applications of personal data processing in day to day activity of companies

With respect to particularities of the application of data protection aspects in the activity of companies and in relation to employees, Article 29 Working Party [4] stated in one of its guidelines [5] that *data protection law does not operate in isolation from labor law and practice, and labor law and practice does not operate in isolation from data protection law. This interaction is necessary and valuable and should assist the development of solutions that properly protect workers' interests* [6]. Consequently, there is a close interconnection between data protection matters and labor law, which reflects in various aspects of the daily activity of a company, as will be further detailed.

3.1. Human resources activities

It is commonly known that any employment context routinely entails processing of employees personal information, including sensitive personal data. Such processing is performed right from the signing of the employment contract or even before this moment, during the recruitment process (as the individuals applying for openings provide the prospective future employer a series of personal information that shall be used by the latter for assessing the merits of the candidate's application and whether they fit the requirements of the particular position) and may continue even after the employment relation ends, if the employer is under a legal obligation to archive former employees' personal information.

This practice is completely motivated, as human resources activities ensure the primary relationship between the employer and the employee and also entail specific attributions of the employer that could not be performed if the latter is not provided access to a series of personal information of the employees (*e.g.* registering the employees in the public registers, drafting the individual employment agreements).

However, even though processing personal information for the HR purposes is reasonable and justified, data protection regulations must still be observed, as unlawful access of other persons to such data may damage the data subject, both materially and morally. Therefore, it is important that the employer completely fulfils all the legal requirements with respect to the modalities in which personal information is processed and the measures it must apply in view of avoiding any *accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, notably if the respective processing involves the data's transmission within a network, as well as against any other form of illegal processing* [7]. Such measures may consist of (i) implementing a security check that permits the identification and the authentication of the user (*e.g.* encrypted passwords), (ii) only allowing certain persons to process the personal data and/or (iii) executing safety copies of personal data, which shall be preserved in secure and restrictive conditions [8].

Furthermore, in performing employees' personal information processing activities, employers must observe certain fundamental data protection principles, such as *transparency* (*i.e.* workers must be informed on various particularities of their personal information processing activities, such as the processing purpose, the existence and the identity of data processors, whether it is mandatory or not to grant access to their personal information and on the existence of certain rights expressly provided by the law to data subjects), *proportionality* (*i.e. personal information must be adequate, relevant and non excessive in relation to the purposes for which they are processed*), *finality* (*i.e.* the purposes of personal data processing activities must be *specified, explicit and legitimate*) or the *awareness of the staff* (*i.e.* the staff whose daily activity implies workers' personal data processing must be trained on data protection regulations) [9].

Within our jurisdiction, the local secondary legislation on data protection matters [10] provides certain particularities with regard to the processing activities of personal information for HR purposes. Hence, in Romania, submission of a notification *is not required when the processing of personal data regarding their own staff and external co-workers is performed by public and private law entities in order to fulfill their legal obligations*. In other words, employers are allowed to process personal information of their employees for the purpose of fulfilling the legal requirements in this field, without being under any obligation to notify such activities with the Data Protection Authority.

Such an approach may raise practical issues in those cases when companies outsource their human resources activity to payroll providers also located in Romania. Hence, the issue is to determine whether the aforementioned exemption also applies in these particular situations, or it only targets the human resources activities that are effectively performed – *in house* – by

the companies. The solution provided in practice to this matter and which we also endorse is that the exemption applies in all the human resources activities performed within Romanian territory, and not necessarily inside the company.

However, the exemption that allows the data controller to avoid notification of data processing shall apply only in those cases when employees' personal information is not transferred abroad for the purposes of performing HR specific activities [11]. Also, the exemption from the obligation to notify personal data processing activities performed for HR purposes does not dismiss the data controller's obligation to observe the other legal obligations incumbent on them pertaining to personal data processing (*e.g.* the obligation to inform the data subject on its personal data processing activities, the processing purpose, the existence and the identity of data processors, minimal security measures) [12].

3.2. Implementation of whistleblowing schemes

Whistleblowing schemes grant the possibility to both public or private entities' employees to report non-observance of internal regulations related to a breadth of scopes expressly provided whether by countries' local applicable legislation, if such legislation was adopted, or by European guidelines [13]. According to the European applicable guidelines, by means of whistleblowing schemes employees may report any concern related to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime [14].

However, the aforementioned guidance is not final as it has been adopted by Article 29 Working Party only for those areas where it was most urgently needed. Further analysis on whistleblowing schemes is necessary to be performed in view of establishing all the aspects of such procedure and determine whether it might be applicable to other fields than those previously mentioned, such as human resources or offences [15].

As regards the particular case of Romania, mention should be made that local legislation only expressly regulates the implementation of whistle blowing schemes within public entities. Hence, private entities willing to adopt such system must refer to the European applicable guidelines in this field. However, application of this procedure in Romanian private entities is rather recent and not very frequent, as whistleblowing systems have only begun to be implemented in our country in the last few years, especially by the local branches of multinational companies, following the example given by their parent companies.

Any person willing to make a report must take into account that reporting the non-observance of internal regulations by means of whistleblowing systems is secondary to notifying such behavior through the usual internal reporting modalities, such as the line management, the competent departments of the employer (*e.g.* human resources, financial) or other such methods. Hence, *whistleblowing should be viewed as subsidiary to, and not a replacement for, internal management* [16]. However, particularities of the whistleblowing schemes, such as the modalities in which persons may file reports, content of a report or prospective actions that shall be performed by the representatives of the companies are established by the data controllers, on a case by case basis.

As regards the protection of the persons implied in the whistleblowing schemes, it is noteworthy to mention that existing regulations mainly focus on the person making the report, namely the whistleblower. Moreover, in the USA or some European countries such as the United Kingdom there are several law firms focusing on the protection of whistleblowers' rights. This approach is understandable and motivated, as submitting a report may attract a negative image of that person within the entity, due to the conservative approach of different nations with regard to such actions of reporting misconducts. As regards the case of Romania, such protection methods were not implemented yet, due to the lack of a relevant legislative framework and also due to the fact that this system has not been yet exploited in its entirety.

However, whistleblowing applicable legislation should also focus on protecting the person incriminated in the report, as it is *stressed that whistleblowing schemes entail a very serious risk of stigmatization and victimization of that person within the organization to which he/she belongs. The person will be exposed to such risks even before the person is aware that he/she has been incriminated and the alleged facts have been investigated to determine whether or not they are substantiated* [17]. The aforementioned risk may be diminished, though, if the data protection rules are properly applied in the reporting process.

As regards such rules, according to the European Directive [18], processing personal data by means of whistleblowing systems can be lawfully performed only if such processing is performed for compliance with a legal obligation or for the purposes of a legitimate interest of the employer or of a third party. Of these two aforementioned conditions, special attention was given to establishing the complete meaning of the notion of *"legitimate interest"*. Thus, according to the Article 29 Working Party [19], in order to be considered as legitimate, the interest must be pursued *in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be 'acceptable under the law'.* [20] Moreover, according to the same European guidelines, in order to be legitimate, the interest must therefore *(i) be lawful (i.e. in accordance with applicable EU and national law), (ii) be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific)* and it must *(iii) represent a real and present interest (i.e. not be speculative)* [21].

As concerns the implementation of whistleblowing schemes in public entities, certain specific provisions shall supplement the other conditions provided above [22]. As such, unlike the provisions of the European applicable guidelines, that only mention an exhaustive list of purposes which may entitle a whistleblower to make a report, Romanian applicable legislation on public entities provides a wide range of such scopes, amongst which can be mentioned the use of whistleblowing schemes for reports having as object abusive use of material and human resources, incompetence and negligence at work, subjective evaluations of personnel in the process of recruitment, selection, promoting, retrograding or dismissing infringement of the legal provisions on public acquisitions and non-refundable financing, as well as for the violation of other legal provisions that require the principle of good administration and the protection of the public interest [23].

However, similar to the European guidelines, Romanian legislation on public entities also focuses on the protection of the person making the report by means of whistleblowing schemes implemented in such entities. Amongst the measures that may be taken for protection such person, there can be mentioned the concealing of whistleblower's identity or, if case may be, even the implementation of other more restrictive measures for protecting the identity of the whistleblower, measures that are usually applied for the protection of witnesses.

In addition to the above, mention should be made that the Data Protection Authority issued an opinion in one of its annual reports of activity that processing personal information by means of whistleblowing systems both in public and in private entities may imply special risks for individuals rights and freedoms and, consequently a prior control may be performed with respect to such activities, in accordance with the law [24].

3.3. Surveillance of employees' electronic communications

The right of every individual to private life [25] includes respecting the privacy of its correspondence and it is a mandatory principle that must be observed within the daily activity of any person. This fundamental right does not only apply in the leisure time, but also during the working program, as different aspects of individuals' private life may also reflect in the professional area.

The subject of establishing whether employers are entitled or not to monitor the electronic communications of their workers has been intensely debated in the last few years, as such practice entails a series of issues which may be addressed by several legal areas of practice, such as criminal law, data protection or civil legislation. Furthermore, the actuality and importance of this subject also determined the Article 29 Working Party to issue an analysis of the consequences that such practice may imply [26].

In the particular case of Romania, mention should be made that our local legislation does not expressly regulate this matter. Consequently, workers surveillance activities performed by Romanian employers shall be performed in accordance with the European guidelines in this field.

For starters, it is necessary to determine which type of actions may be considered "workers electronic communications". Hence, Article 29 Working Party considers that the aforementioned expression mainly refers to personal emails and the use of Internet for personal purposes, performed at the workplace, by using employer's logistics.

As regards email monitoring, it has been unitary established both within the guidelines issued by the Article 29 Working Party [27] and within the jurisprudence of the European Court of Human Rights [28] that *electronic communications made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 of the European Convention* [29] and, consequently, benefit by all the protection that law grants to the aforementioned notions. In other terms, it is not forbidden to execute surveillance activities of such communications, as long as they are performed in accordance with the applicable provisions on the protection of private life.

With respect to the private use of Internet at work, there is not any unitary or at least majority opinion whether there should be permitted or not to the employer to monitor such use. Hence, companies may decide, on a case by case basis, whether they shall monitor the use of Internet by its employees or not. However, if an employer decides that it shall perform Internet use monitoring activities, certain mandatory rules must still be observed.

Hence, in cases when employers decide to monitor their workers' use of Internet, the latter must be informed on this aspect. This is an application of the transparency principle that is detailed below.

However, it is recommendable that, instead of focusing on the monitoring of Internet use, the employer should implement technical measures to restrict employees' access to certain websites. This would bring even more benefits to the employer and would help the latter streamline its activity, as such measure would resolve employee's lack of efficiency caused by excessive Internet use, instead of resolving its effects, which may consist, for instance, of losses in the profit of the company as a result of the inefficient activity of the workers. In other words, *prevention should be more important than detection* [30].

If the employer decides to monitor the Internet use by its workers, it should at least attempt to gain access to a lesser amount of employee's personal information as possible, in order to give effect to the proportionality of such measure. Therefore, in order to violate as less as possible employee's right to privacy, the employer should focus on collecting data regarding the duration of such internet use or the general category of targeted websites, instead of collecting detailed personal information on the content of the websites visited.

In addition to the above, there are a series of principles that any employer must observe both in cases when it processes personal data by means of email monitoring and by means of Internet private use monitoring.

Thus, a first aspect that must be analyzed consists of assessing the **finality** of workers' electronic communications surveillance and whether this surveillance is **necessary, legitimate** and **proportionate** with the purposes that the employer wishes to achieve further to such actions. Hence, employers may process their workers' personal information by means of such

communications surveillance methods only for *a specified, explicit and legitimate purpose and* this information shall not be *further processed in a way incompatible with those purposes* [31]. In order **to be compatible** to the processing purposes, the personal data that is collected by means of electronic communications surveillance must only be used for such purposes. For instance, if an employer supervises the communications of an employee due to the fact that it was informed that the employee reveals confidential aspects regarding employer's activity to third parties, any personal data collected within this process may only be used for establishing whether the employee breached its confidentiality obligation or not. This data shall not be used for other purposes, like assessing the professional performances of the data subject.

Moreover, in order to be **proportional** and **necessary**, communications' surveillance must be performed in view of protecting an employer's right or interest. Such right or interest must prevail over the right of the employee to privacy. This may be the case of employer's right or interest to streamline its business, to protect itself from any actions performed by its workers and which may also entail its civil responsibility in accordance with the applicable legal provisions or to reduce negative and prejudicial effects that may be entailed when a criminal offence is committed by an employee against the employer.

More than that, according to the Article 29 Working Party, in order for the principle of proportionality to be observed, *the monitoring of emails should, if possible, be limited to traffic data on the participants and time of a communication rather than the contents of communications if this would suffice to allay the employers concerns. If access to the e-mail's content is absolutely necessary, account should be taken of the privacy of those outside the organization receiving them as well as those inside* [32].

This point of view raises another concern entailed by such email monitoring activities, namely the fact that, by accessing the content of employees' emails, employer shall also collect personal information of the sender/receiver from outside the company. Thus, data protection regulation, such as the right to be informed on its personal data processing activities, should also apply to the latter. In practice, this might be rather difficult to achieve, and therefore may entail the risk for the employer of breaking the sender/receiver's rights provided by the data protection regulation with respect to the processing of its personal data.

In performing monitoring activities, the employer must also observe the principle of **transparency**. This principle consists of two obligations incumbent to the employer, namely (i) the obligation to inform the employee about the fact that its emails and Internet use are monitored and (ii) the obligation to notify the competent data protection authority with respect to the personal data activities it performs. As regard the first obligation, Article 29 Working Party provides that *the employer has to provide his workers with a readily accessible, clear and accurate statement of his policy with regard to e-mail and Internet monitoring* [33]. These obligations are also expressly provided within the Romanian legislation for any kind of personal data processing activities.

With respect to the activities performed by Romanian data controllers and which consist of employees monitoring, including surveillance of their use of Internet, it is worth mentioning that the Data Protection Authority' representatives already performed controls targeted on such activities. For instance, of greater interest for the case at hand, is a control conducted on the activity of processing employees' personal data performed by means of a software application installed on their working stations and which aimed to monitor especially the duration for which they were effectively performing working activities. Such application permitted the employer to collect data such as the volume of printed documents, the applications and site that is used by the employee or the period of time in which the system was used. The collected personal data were transferred in the USA, on the servers of the entity that owned the application. However, the representatives of the Data Protection Authority ascertained that the data controller failed to fulfill the legal obligation to submit a notification with respect to the processing activities it performs, it did not observe its legal obligation to inform data subject with respect to such processing activities and it also did not offer any adequate guarantee for the transfer of the personal information in the USA. Therefore, it was applied a fine, in accordance with the law [34].

3.4. Video surveillance of employees

The technological progress that is becoming more and more accelerate in all the fields of the contemporary life has lead to an increasing proliferation of video systems, as well as other digital tools that are used for a wide range of purposes. Among these purposes it is worth mentioning the use of video systems for the protection/monitoring/security of persons, locations and/or public/private assets.

Such video surveillance methods entail a series of data protection issues, as they imply collecting a great amount of personal information concerning identified/identifiable individuals (*e.g.* their image, behavior, habits or even their voice). Therefore, it is deemed that illegitimate, inadequate or excessive use of such systems may cause serious prejudices to the fundamental rights and liberties of individuals. According to European applicable guidelines [35], among such rights that may be prejudiced by means of video systems use is the free movement of individuals, which consists of the right of *everyone lawfully within the territory of a State to, within that territory, have the right to liberty of movement* [36], *without undergoing excessive psychological conditioning as regards their movement and conduct as well as without being the subject of detailed monitoring on account of the disproportionate application of video surveillance by several entities in a number of public and/or publicly accessible premises* [37].

Any data controller processing personal information by means of video systems must ensure that it has implemented all the necessary technical measures for providing the security of the personal information collected by means of the video cameras and, as well, that is performs these activities in accordance with the mandatory provisions of the European applicable legislation [38]. Hence, according to the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**Data Protection Directive**"), *the images collected by means of video systems must be processed fairly and lawfully, for specified, explicit and legitimate purposes* [39]. *Furthermore, the personal data collected must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed* [40].

As regards the particular aspects of employees' personal information processing activities performed by means of video systems, Opinion 4/2004 of Article 29 Working Party provides that processing personal information of employees by means of video systems *aimed directly at controlling the quality and amount of working activities should not be permitted* [41]. On the other hand, such rule does not apply when video systems are installed *to meet production and/or occupational safety requirements and also entail distance monitoring* [42].

In Romania, special legislation on video surveillance [43] provides a series of mandatory conditions that must be fulfilled by data controllers that process personal information by means of CCTV systems.

First of all, it is necessary to clearly define which of the information captured by the video cameras may be considered "personal data". Hence, the Romanian competent authority on data protection aspects has established that *any images of identified or identifiable persons, that are processed by means of video surveillance, may be considered personal information* even in those cases when *they are not associated with an individual's identification data* or even if *they do not contain the image of the filmed person, but other information which may lead to the identification of the aforementioned person (e.g. vehicle's registration number)* [44]. Therefore, in practice, when images collected by the video cameras are made available to third parties, individual's face as well as any other information that may lead to the identification of individuals is blurred.

In addition to the above, the CCTV systems *must be installed in visible places* [45] and must be accompanied by an icon informing persons on the fact that they may be video-recorded. Hence, installing hidden cameras or using such systems in place where persons intimacy should be granted (*e.g.* fitting rooms, showers) is forbidden.

The personal information collected by means of CCTV systems cannot be stored for more than 30 days as of the date they were video-recorded, except those situations expressly regulated within the law or any other duly justified cases [46].

As regards the processing of personal information of employees at the employer's premises by means of CCTV systems, apart from the aforementioned rules, law provides a series of even more restrictive conditions that must be fulfilled by the date controller. Hence, processing employees' personal information by means of video systems can only be performed in two limitative situations, namely (i) on the basis of employees' consent or (ii) for the view of fulfilling whether an express legal obligation or a legitimate interest.

Employees' consent on being supervised by means of CCTV systems must be express and freely given. Furthermore, employees' rights, such as right to be informed or the right of intervention, which are expressly provided by the law for any individual whose personal data is processed, must always be respected.

However, it is very important to make the distinction between employees' video surveillance and the installing of CCTV systems in those places where employees effectively develop their activity. Hence, employees' video surveillance consists of installing CCTV systems at the entrance of the premises, on hallways, staircases or in any other public places within the company. Such systems can be installed in the aforementioned places if the conditions provided above are fulfilled. As regards installing of CCTV systems in those places where employees effectively perform their working activities, the rule is that such surveillance is forbidden.

In addition to the above, the Romanian Data Protection Authority also issued a supplementary opinion with regard to the processing of employees personal information by means of video surveillance. Hence, apart from the aforementioned conditions, the authority states that it is necessary for the data controller to also observe the provisions of the Labor Code and to provide a strong justification for implementing such measure, concomitantly to consulting the trade unions or the employees' representatives [47].

As regards practical aspects of these regulations, mention should be made that in Romania, Data Protection Authority already applied a series of fines to employers that were processing personal information of their employees by means of video cameras. For instance, Authority's representatives controlled and sanctioned a data controller that was processing personal data of its workers by means of CCTV systems installed at the entrance of the premises, on hallways, but also in employees' offices, without their prior consent and also without being under the incidence of any legal provision that may entitle it to install CCTV systems inside the offices. Nevertheless, the workers were only partially informed on the existence of the cameras, as they were only aware that such cameras were installed on hallways and at the entrance [48].

Another practical case from our jurisdiction derives from a request submitted to the Data Protection Authority by an employer to be granted the approval to process its employees' personal information by means of video systems. Its request was rejected, for a series of arguments, namely: (i) even though the data controller declared that the purpose of installing video cameras at its premises was not to monitor the correctitude and the efficiency of its employees, the employer aimed to install video cameras in the offices, which would have led exactly to such employees' efficiency monitoring; (ii) the employer could not prove that it consulted the trade union or the representatives of the employees prior to taking the decision to install the CCTV systems and (iii) it resulted no concrete cases when employees performed criminal offenses that also prejudiced the employer, in which case its interest to install the video system would have been legitimate [49].

The restrictions imposed by the law to any data controller that processes personal information of individuals by means of CCTV systems are truly motivated, considering the fact that the common practice for entities was to use CCTV systems for monitoring their employees, especially with regard to their correctitude and efficiency of their activity, thus leading to a serious violation of such persons' fundamental right to private life.

4. Practical aspects concerning the activity of the Data Protection Authority

Romanian Data Protection Authority is an autonomous and independent public authority that aims to protect individuals' fundamental rights and freedoms that may be breached during the processing activities of their personal data [50].

One of the main attributions of the Data Protection Authority consists of monitoring and control of the data processing activities performed whether by Romanian data controllers or by foreign data controllers that process personal information by any means located on the Romanian territory, for the view of establishing if such data processing activities are legally performed [51].

Such controls are performed *ex officio* and they are usually carried out in campaigns targeted against entities that have similar objects of activity. However, law also grants the possibility to any individual that considers its data privacy rights were violated by means of illegal personal data processing to submit a complaint to the Data Protection Authority in this regard. If further to a preliminary analysis of the motives provided within the complaint the representatives of the Data Protection Authority consider that further investigations are necessary, they shall conduct a control on the data processing activities performed by the data controller which is subject to that complaint.

The monitoring and control activity conducted by the representatives of the Data Protection Authority materializes in applying sanctions to the data controllers that indeed perform illegal data processing activities. Thus, they may (i) ascertain that such activities are minor offenses and, consequently, apply a fine ranging between EUR 110 to EUR 5,500, if the illegal action of the data controller is not performed in such a manner that may constitute a criminal offense [52], (ii) rule the provisory suspension or cessation of the data processing activities, the partial or integral erase of the processed information or they may (iii) notify the criminal prosecution bodies or file complaints to a court of law [53].

Results of the monitoring and control activity are summarily provided within Data Protection Authority's annual reports of activity. According to such reports, the monitoring and control activity of the Data Protection Authority significantly developed from a year to another.

Lately, in practice, controls become more and more numerous every year as the representatives of the Data Protection Authority are performing a wide activity of monitoring and control, especially in the contemporary context, when protection of personal information against unlawful disclosure and use is one of the most serious concern of data controller, both within the public and the private field.

5. Final Word

It is well known that the daily activities of a company imply processing of a wide range of personal information, for various purposes. Whether for developing the normal activity of the company or for other specific scopes imposed by the contemporary reality and by the necessity and expectation of any company to reach or even to overrun a certain level of development and modernization, access of companies to personal information of its workers and collaborators is essential.

However, such processing activities may only be performed while observing the applicable legislation in this field, while always keeping the fine balance between the legitimate interest of the data controller and the data subject's right to private life.

---

1 Article 2 paragraph 2 of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data

2 Article 2 paragraph 3 of Law no. 677/2001

3 Article 29 paragraph 1 of Law no. 677/2001

4 Independent organism with an advisory status that was set up under the 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

5 Opinion 8/2001 on the processing of personal data in the employment context

6 Opinion 8/2001, page 4

7 Article 20 paragraph 1 of Law no. 677/2001

8 Order No. 52 on approving the minimum safety requirements for personal data processing

9 Opinion 8/2001 of Article 29 Working Party on the processing of personal data in the employment context

10 Decision 90/2006 of the National Supervisory Authority for Personal Data Processing on the situations in which the notification for personal data processing is not required

11 Article 29 paragraph (3) – Personal data transferred to another state shall always be subject to prior notification to the supervisory authority.

12 Article 12 of Law no. 677/2001

13 Opinion 1/2006 of Article 29 Working Party on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime

14 Opinion 1/2006 of Article 29 Working Party

15 Opinion 1/2006 of Article 29 Working Party

16 Idem, page 6

17 Opinion 1/2006 of Article 29 Working Party, page 7

18 Article 7 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

19 Opinion 06/2014 of Article 29 Working Party on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

20 Idem, page 25

21 Ibidem, page 25

22 Law no. 571/2004 on protection of personnel in public authorities, public institutions and other units, who report violations of the law

23 Article 5 of Law no. 571/2004

24 The annual report of activity issued by the Data Protection Authority for 2013

25 Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms - Everyone has the right to respect for his private and family life, his home and correspondence.

26 Working Document on the surveillance of electronic communication in the workplace

27 Working document on the surveillance of electronic communication in the workplace and Recommendation 3/97 – Anonymity on Internet

28 Case Halford *versus* the United Kingdom

29 Working document on the surveillance of electronic communication in the workplace, page 20

30 Idem, page 24

31 Working document on the surveillance of electronic communication in the workplace, page 14

32 Idem, page 17

33 Working document on the surveillance of electronic communication in the workplace, page 14

34 The annual report of activity issued by the Data Protection Authority for 2013

35 Opinion 4/2004 of Article 29 Working Party on the processing of personal data by means of video surveillance

36 Article 2 paragraph 1 of the Protocol no. 1 of the European Convention on Human Rights

37 Opinion 4/2004, page 6

38 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

39 Article 6, paragraph 1, letters a) and b) of Directive 95/46/EC

40 Article 6, paragraph 1, letter c) of Directive 95/46/EC

41 Opinion 4/2004, page 25

42 Idem

43 Decision no. 52/2012 of the Romanian Data Protection Authority on the processing of personal data using video surveillance means

44 Article 1, paragraph 2 of Decision no. 52/2012

45 Article 5, paragraph 2 of Decision no. 52/2012

46 Article 14, paragraph 1 of Decision no. 52/2012

47 The annual report of activity issued by the Data Protection Authority for 2012

48 The annual report of activity issued by the Data Protection Authority for 2013

49 The annual report of activity issued by the Data Protection Authority for 2014

50 Law no. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing

51 Law no. 677/2001

52 Articles 31-34 0f Law no. 677/2001

---

*Iulian Popescu is a partner in the Corporate & Commercial Practice in the Bucharest office of Musat & Asociatii Attorneys at Law. Mr. Iulian Popescu can be contacted at iulian.popescu@musat.ro.

Iulian Popescu
Musat & Asociatii
iulian.popescu@musat.ro
Telephone : +40 21 202 59 28
Fax : +40 21 223 04 95
www.musat.ro/attorneys/partners/iulian-p....html
View profile Download vcard

Posted: Friday, January 1, 2016

Topics: Cyberspace Law / E-Commerce / Internet Law