Data Privacy Alert

22 January 2016

Articles in this issue:

Changes regarding the notification of personal data processing

The Decision of the National Supervisory Authority for Personal Data Processing no. 200/2015 dated 28.12.2015 brings a significant change in connection with the obligation to notify the authority of personal data processing, respectively this will become the exception in the cases expressly provided under the law.

Is it legal to access your employees' communications? European Court says "yes, but only in exceptional cases"

On 12 January 2016, the European Court of Human Rights issued its judgment in the case of Bărbulescu v Romania and decided that, although privacy should be respected at the workplace, the employers may be entitled to access their employees' private correspondence but only in very particular circumstances.

Changes regarding the notification of personal data processing

The Decision of the National Supervisory Authority for Personal Data Processing (the "**Authority**") no. 200/2015 (the "**Decision**") was published in the Official Gazette no. 969/28.12.2015.

The change in the legal regime regarding the notification of the Authority

The main amendment brought to the specific legal framework governing personal data processing through the Decision is the change in the legal regime regarding the notification of the Authority.

According to the Decision, the notification to the Authority regarding personal data processing will become an **exception**, being applicable only in the cases expressly stated by law and mentioned below, while the general **rule** would be that personal data processing is allowed without any other prior notification.

This new legal regime does not exempt the data controller from its other obligations based on Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, especially obligations to protect the rights of the persons in cause, the confidentiality and security of data.

Notification of data processing cases to the Authority

The exceptions mentioned below for which the obligation to notify the Authority will still be applicable are justified either by the nature of the criteria on which the data processing is performed, or in consideration of certain qualities of the individual whose personal data are processed or taking into consideration the way in which the data is collected:

1. Processing personal data related to ethnical or racial origins, political, religious, philosophical or other similar beliefs, union affiliation, as well as data regarding health conditions or sex life;
2. Genetic and biometric personal data processing;
3. Personal data processing which allows directly or indirectly geographical localisation of natural persons through electronic communication devices;
4. Processing minors' personal data, if such activity was performed:
    - during direct marketing activities;
    - via internet or electronic messages;
5. Personal data processing regarding the perpetration of an offence by the person in cause or regarding criminal convictions, preventive measures or administrative or minor offences' sanctions applicable to the person in cause, performed by private law entities;
6. Personal data processing via electronic devices aiming to monitor and/or evaluate aspects such as personality, professional capacity (competence), credibility, behaviour or other similar aspects;
7. Personal data processing via electronic devices within evidence systems aiming to take automatic individual decisions relating to the evaluation of solvability, financial and economic situation, actions which may imply disciplinary, minor offences' or criminal liability of natural persons by private law entities;
8. Personal data processing via video surveillance systems, including the transfer of such data to a non-EU state.

Exceptionally, the notification of the Authority for the case where the personal data processing is performed by an individual in his/her own personal interest will not be necessary, even if the images saved also comprise public domain pictures.

However, the **general rule will be applied**, meaning that it will not be necessary to notify the Authority, even in one of the **above mentioned situations**, if one of the following situations are applicable:

1. Personal data processing is provided by law (e.g. credit institutions);
2. Personal data processing is performed in view of the transfer abroad based on a special law or an international treaty ratified by Romania;
3. Personal data processing is performed exclusively for journalistic, literary or artistic purposes, if the data was made public manifestly by the person in cause or they are related to the public person quality of the individual in cause or by the public characteristic of the actions in which he/she is involved.

The time when the notification of the Authority must be performed

The operator has to notify the Authority of the personal data processing prior to the actual processing.

At the same time, if the personal data processing falls within the situations mentioned at points 1, 2, 5 above, the Authority will order a prior control. In case the Authority does not inform the data controller regarding the control within 5 days of the notification, the data controller will be able to proceed with the personal data processing.

Transfer of personal data outside the EU

The transfer of personal data to countries outside the European Union, European Economic Area, as well as to countries for which the European Commission has not recognised by decision an adequate level of protection will continue to be notified to the Authority.

In addition, such transfers will require prior authorisation by the Authority.

Is it legal to access your employees' communications? European Court says "yes, but only in exceptional cases"

On 12 January 2016, the European Court of Human Rights (the "Court") issued its judgment in the case of Bărbulescu v Romania, pursuant to application no. 61496/08. In this decision, the Court ruled that, although there is privacy at the workplace and employers have no legal right to track their employees' communications, such an interference might be acceptable in certain conditions.

The relevant facts

Mr. Bărbulescu was in charge of sales for a private company, for which purpose he was instructed by his employer to create a Yahoo Messenger account. As regards this account: (i) it was a Yahoo Messenger account having as purpose chat communication, (ii) it was created by the employee at the request of the employer for the purpose of responding to clients' enquiries and (iii) the employee declared that he was using the account only for professional purposes (both under the internal regulation and at the separate request of the employer).

In order to check the manner in which professional tasks of Mr. Bărbulescu were completed, the employer had monitored Mr. Bărbulescu's Yahoo Messenger account from the company's computer. Furthermore, the employer alleged that Mr. Bărbulescu, by using the company's computer and the account he was instructed to create, for personal purposes, had breached express provisions assumed under the internal regulation, and thus, the employer terminated Mr. Bărbulescu's contract.

The decision to terminate the contract was challenged by Mr. Bărbulescu before the competent Romanian courts, alleging that the employer had breached the applicant's right to private life and specifically, secrecy of correspondence. The Bucharest Court of Appeal finally ruled that, since the employee claimed during disciplinary proceedings that he had not used Yahoo Messenger for personal purposes, the employer was entitled to check the content of communication, as this was the only method for the employer to verify the defense.

Mr. Bărbulescu complained in front of the Court that his employer's decision to terminate the contract had been based on a breach of his right to respect for his private life and correspondence, protected under Article 8 of the European Convention on Human Rights.

The Court's assessment

1. In line with its constant case law, the Court considered that communications through Yahoo Messenger account should be included in the notion of "private life" and "correspondence" under Article 8 of the European Convention on Human Rights;

2. In the absence of a warning from the employer that such communications are subject to monitoring, an employee would have a reasonable expectation of privacy when communicating from a work related device. Also in the specific situation of Mr. Bărbulescu, the Court examined whether the applicant had a reasonable expectation of privacy when communicating from Yahoo Messenger account that he had registered at his employer's request, even if the internal regulations of the employer prohibited the use of company assets for personal purposes;

3. **The Court examined whether the right to respect for private life and correspondence is balanced with the employer's interest and decided that the employer had a legitimate interest because the following reasons were cumulatively met:**

    - the communications of the applicant were only accessed in the framework of disciplinary proceedings, as a result of the applicant's own allegations of not using the Yahoo Messenger account for personal purposes;

- the monitoring itself was limited to the Yahoo Messenger account, not extending to other communications from that account or other records from the computer;
- the domestic courts did not attach particular weight to the actual content of the applicant's communications, they relied on the transcript only to the extent that it proved the applicant's disciplinary breach, namely that he had used the company's computer for personal purposes during working hours. There was no mention in their decisions of particular circumstances that the applicant communicated; the identity of the parties with whom he communicated is not revealed either;
- the applicant did not convincingly explain why he had used the Yahoo messenger account for personal purposes.

Conclusion

The Court concluded that although there is privacy at the workplace and employers have no legal right to track their employees' communications, such an interference might be acceptable if the right to respect for private life and correspondence is balanced with the employer's interest. In case of Mr. Bărbulescu the communications of the applicant were accessed in order to check the manner in which professional tasks of Mr. Bărbulescu were completed, in the framework of disciplinary proceedings, as a result of the applicant's own allegations of not using the Yahoo Messenger account for personal purposes.

Kindly note that the Court's decision is linked to a specific situation, and Court's conclusions should be read in the light of the cumulative particularities of the case. Please be aware that the monitoring of the employee's communication by the employer was neither a preventive measure nor a continuance one. Thus, this decision cannot be invoked as such in other similar situations and a full assessment of the concrete situation is necessary to be made on a case by case basis.

Implications and next steps

Considering the circumstances of the case, to the extent that employees' activity is being monitored at the level of your company, the following aspects should be taken into consideration, among others, the following aspects:

- The internal policy or regulation should include details relating to monitoring (reasons, circumstances etc.);
- Clear rules should be set forth regarding the type of monitoring and the number of persons that can verify and monitor employees' activity should be limited;
- The conditions of necessity and proportionality of the measure should be verified, in relation to the specific situation at hand.

If you have questions or you want more details regarding the inward processing procedure and how to apply for it, please do not hesitate to contact us.

Andrei Burz-Pinzaru
Partner Reff & Associates
Attorney at Law
+40 21 207 52 05

Andrei Ionescu
Partner, Deloitte Risk Advisory
+40 21 207 54 85

Florentina Munteanu
Associate Partner Reff & Associates
Attorney at Law
+40 21 207 52 75

Cătălina-Teodora Stroe
Manager, Deloitte Risk Advisory
+40 21 222 16 61

Maria-Silvia Axinescu
Managing Associate Reff & Associates
Attorney at Law
+40 21 207 54 28