TUCA ZBARCEA
ASOCIATII

Issue 15, June 2016

Just in Case

An online publication of Țuca Zbârcea & Asociații

In this issue

Table of Contents

Intro

Personal Data: The New "Oil" of The Digital Economy

Personal Data: The New "Oil" of The Digital Economy

Modern society is experiencing an unprecedented "data boom", fundamentally altering and adding sophistication to all human activities, which are thus becoming ever more information-driven. Numerous studies convincingly show that such "data universe" in full expansion impacts businesses (which need to understand and adjust to a dynamic environment), as well as consumers (which are both the fundamental source and the ultimate beneficiaries of shifting commercial trends). In 2012, The Boston Consulting Group estimated that the volume of global data transactions increases annually by 45%, which means that the data volume doubles every one-and-a-half years.

As a relevant dimension of this process, the history of internet browsing indicates that the total internet traffic has experienced an outstanding growth in the past two decades. In 1992, global internet networks carried approximately 100 GB of traffic per day. In 2002, that amounted to 100 GB per second, while in 2015 global internet traffic reached more than 20,000 GB per second[1].

This data and information revolution brings about new economic, social and ethical challenges, as individuals become not only consumers, but also providers of a very valuable asset: their personal data, often referred to as "the new oil" which the industry is keen to process for powering-up lucrative operations. As illustrative as this comparison may sound, one must keep in mind that personal data is not a resource waiting to be harvested and exploited. Use of personal data needs to be calibrated so as to ensure the protection of fundamental rights, especially privacy and data protection, without affecting economic expansion.

On the one hand, consumers whose data are harvested by the industry have a legal right that their personal data be used for legitimate purposes, which the consumers are duly and timely made aware of. Consumers expect that, when handling their personal data, the industry makes sure such data is protected against misuse. Statistics show however that there are considerable worries about privacy, and these worries can negatively affect the business.

On the other hand, given the high commercial potential of personal data, the industry may see rules on protection of personal data as an obstacle to their development.

This social and economic environment requires public policy makers to create a legal framework>

1. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

which would allow the industry to use personal data in a sound and fashionable manner, so as to protect the legitimate interests of the data subjects. Finding the right balance between the legitimate expectations of data subjects and those of the industry is crucial, and the legal framework needs to set the stage for mutual trust between the two sides.

In 2012, the European Commission launched a comprehensive reform of data protection rules in the EU. The official texts of the new legal framework in the field were published and are expected to be applicable starting with May 2018. It is the intention of the Commission to empower individuals to reclaim control over of their personal data, to simplify the regulatory environment for business, and to enable European citizens and businesses to fully benefit from a digital economy[2].

In any case, no matter how much the new regulatory rules succeed in bridging data subject's rights and the industry's interests, trust needs to be earned through sound commercial policies, able to show that protection of personal data is a priority for the industry also. Needless to say, data protection creates significant costs to the industry; according to an impact assessment prepared in 2013, the EU data protection framework imposes on European companies an administrative burden totalling EUR 5.3 billion[3]. Despite that, companies need to understand the importance of the matters and adopt policies that would ensure protection of personal data.

Also, while e-commerce made significant inroads into the hearts and minds of a new generation of consumers, the electronic environment is yet to become a safe-haven for consumers' data and money. With cyber-attacks becoming ever-more sophisticated, the industry must invest significant resources in the security of the data they are processing.

Not least, protection of personal data needs to be factored-in when designing employment policies. Employers have to adopt proper regulations ensuring that their employees feel protected and respected, and that monitoring employees' performance at the job does not intrude on their personal life.

All these challenges increase the importance of personal data protection for the actors involved. "Data" got "Big", so that data protection rapidly emerged from a marginal topic into a mainstream concern for data subjects, industry, policy makers and legal experts.

Bogdan Halcu,
Managing Associate
bogdan.halcu@tuca.ro

2. http://ec.europa.eu/justice/data-protection/
3. http://www.ivir.nl/publicaties/download/1350

Case by Case

Moving Data Centres to Romania: The Do's and Don'ts

Moving Data Centres to Romania: The Do's and Don'ts

In recent years, Romania has become a more prominent investment location for data centre providers on account of country's sustained economic growth, the proliferation of the IT&C infrastructure, coupled with Romania's highly skilled workforce in the IT&C industry and the overall lower operating costs as compared to other countries.

Drawing upon our team's extensive expertise in data protection applicable regulations affecting various industries, a number of foreign data centre providers retained Țuca Zbârcea & Asociații for advice on the legal implications of moving data centres/ servers to Romania.

When prospecting the idea of locating data centres / servers in Romania, services providers should take into account that certain regulatory requirements may apply, especially those concerning data protection/security, including the rules on the governmental access to data.

We shall briefly outline below a few of the most common regulatory issues raised by our clients, together with a few recommendations in connection thereto.

How to Determine Whether Romanian Data Protection Law Applies

Law No. 677/2001 on processing of personal data shall apply to data controllers not based in Romania to the extent they use equipment, automated or otherwise, located on Romanian territory, unless such equipment is only used for transiting the data through Romanian territory. These provisions seem conflicting with the provisions of the EU Data Protection Directive, under which national law becomes relevant when data controllers established in a non-EU Member State make use of equipment situated on the territory of EU Member States. This inconsistency between the national law and the EU directive may be explained by the fact that Law No. 677/2001 was enacted before Romania's accession to the EU.>

of harmonised data protection rules throughout EU countries, which justified the limitation of the cross-border scope of national laws for the processing carried out by controllers established in EU Member States, and undertakings processing in other EU Member States.

Although the provisions of Law No. 677/2001 were not formally amended, one may construe that, starting with Romania's accession to the EU, the aforementioned national provisions of the applicable law should be read by reference to the EU Data Protection Directive. Even though no official decision / act was issued, such approach appears to be shared in practice by the Romanian data protection authority.

Therefore, when considering using data centres located in Romania, foreign data controllers should take into account the following rules as regards the applicable law:

- Processing activities carried out by data controllers established in other EU countries will continue to be governed by the laws of the EU country where such entity is established; and;
- Processing activities carried out by a non-EU data controller will be governed by the Romanian data protection legislation.

When a foreign data centre owner does not qualify as data controller, but as a data processor (e.g. will act merely as cloud provider), it will not be directly bound to comply with the Romanian data protection legislation. However, if the customer is a Romanian entity acting as a data controller (e.g. cloud customer), the service provider will have to indirectly comply with the Romanian legal framework. That is because the customers usually request the provider, under the contract, to comply with the Romanian data protection laws and standards (or, if the provider is an EU-based entity, with the EU data protection laws and standards).

Data Security and Cloud Computing

Data security is one of the most common issues listed in connection with the use of cloud computing.

According to Article 21(3) of Law No. 677/2001, cloud customers should choose cloud providers implementing adequate technical and organisational security measures to protect personal data, and who are able to demonstrate accountability, which means ensuring availability (reliable access to personal data), integrity (data is authentic and has not been maliciously or accidentally altered), confidentiality (by appropriate means such as encryption, authorisation mechanisms and strong authentication), transparency, purpose limitation, inevitability (the cloud provider and the subcontractors are obliged to support the customer in facilitating the exercise of data subjects' rights), portability and responsibility (reliable monitoring and comprehensive logging mechanisms).>

> " Data security may be ensured not only by contractual safeguards, but also by way of factual safeguards.

Cloud customers (i.e. usually the data controllers) are aware of the importance and advantages of secured cloud services. Therefore, any risks related to data security breaches are usually covered under specific contractual safeguards, such as:

- Specifying the security measures that the cloud provider must comply with, depending on the risks arising out from the processing and on the nature of the data to be protected;
- Subject and time frame of the cloud service, extent, manner and purpose of the processing of personal data by the cloud provider, as well as the types of personal data processed;
- Conditions for returning the (personal) data or destroying it once the service is concluded;
- Confidentiality clauses;
- Prohibiting the disclosure of data to third parties, except for subcontractors specifically allowed under the data processing agreement;
- Cloud provider's responsibility to notify the cloud customer, in the event of any data breach which affects the cloud client's data; etc.

Data security may be ensured not only by contractual safeguards, but also by way of factual safeguards. Therefore, the cloud customer(s) will thoroughly verify the selected cloud vendor(s)'s data security policy, as well as the track record of dealing with past security incidents (if any). Such verification may refer not only to potential security incidents, but also to how they were handled, how fast the security breaches were notified and remedied, and what measures have been implemented by the cloud provider in order to prevent recurrence thereof.

Where sensitive data is involved (meaning any data subject to a special regime, be it commercial secret, banking secret or other), factual security measures may be a keystone of the cloud customer's choice in favour of a certain cloud service provider. Therefore, a solution which is highly recommended by the industry, and also more frequently sought by cloud customers, is the unidirectional encryption of data. Although the encryption services are usually required from a third party, encryption services provided by the cloud providers themselves are well-appreciated by cloud customers (as they guarantee the reliability of the services rendered by the could provider).

Compliance With Law Enforcement Disclosure Requests

Nowadays, various governmental authorities throughout the world are aiming to gain more control and access to data which is stored by/in possession of various services providers (e.g. cloud providers, internet content providers).

Therefore, service providers are more and more concerned to clarify the means of protecting the individuals' private life (including from the government's illicit intrusion), but also to ensure compliance with the relevant legal framework.

The most common issues raised by our clients in this respect may be summarised as follows:

- **Competent bodies allowed to request access to data** - under the Romanian Code of Criminal Procedure, any private individual or legal entity on Romanian territory is bound to disclose, at the request of the enforcement bodies (namely, prosecutors, criminal investigation bodies of the judicial police and special crime investigation units) and the courts of law, the communications data held in their possession or under their control, which are stored on computer systems or communications data storage media. Furthermore, the private individual or legal entity should allow the law enforcement bodies: (i) to access their premises, and (ii) to install the law enforcement bodies' own equipment and/or (iii) to access their local servers;
- **Disclosure of encryption keys** - although there is no express reference to encryption keys (e.g. necessary for accessing certain data stored on the servers), in light of the broad obligation to make available any communications data, it can be reasonably construed that such data also entails the obligation to provide the required means to make the data readable and enable the law enforcement bodies to use the data;
- **Means to challenge the data access request ordered by Romanian bodies** - providers should be aware that an illegal/abusive request for information made by the law enforcement bodies may be challenged by means of a complaint settled by the chief prosecutor of the prosecutor's office investigating the criminal case. Furthermore, we note that a request of information under a non-legal process is not>

allowed. The law enforcement bodies are entitled to request and obtain the disclosure of such information only by complying with a specific legal process which essentially requires the issuance of an order by a criminal prosecution body or an order/decision of a court of law;

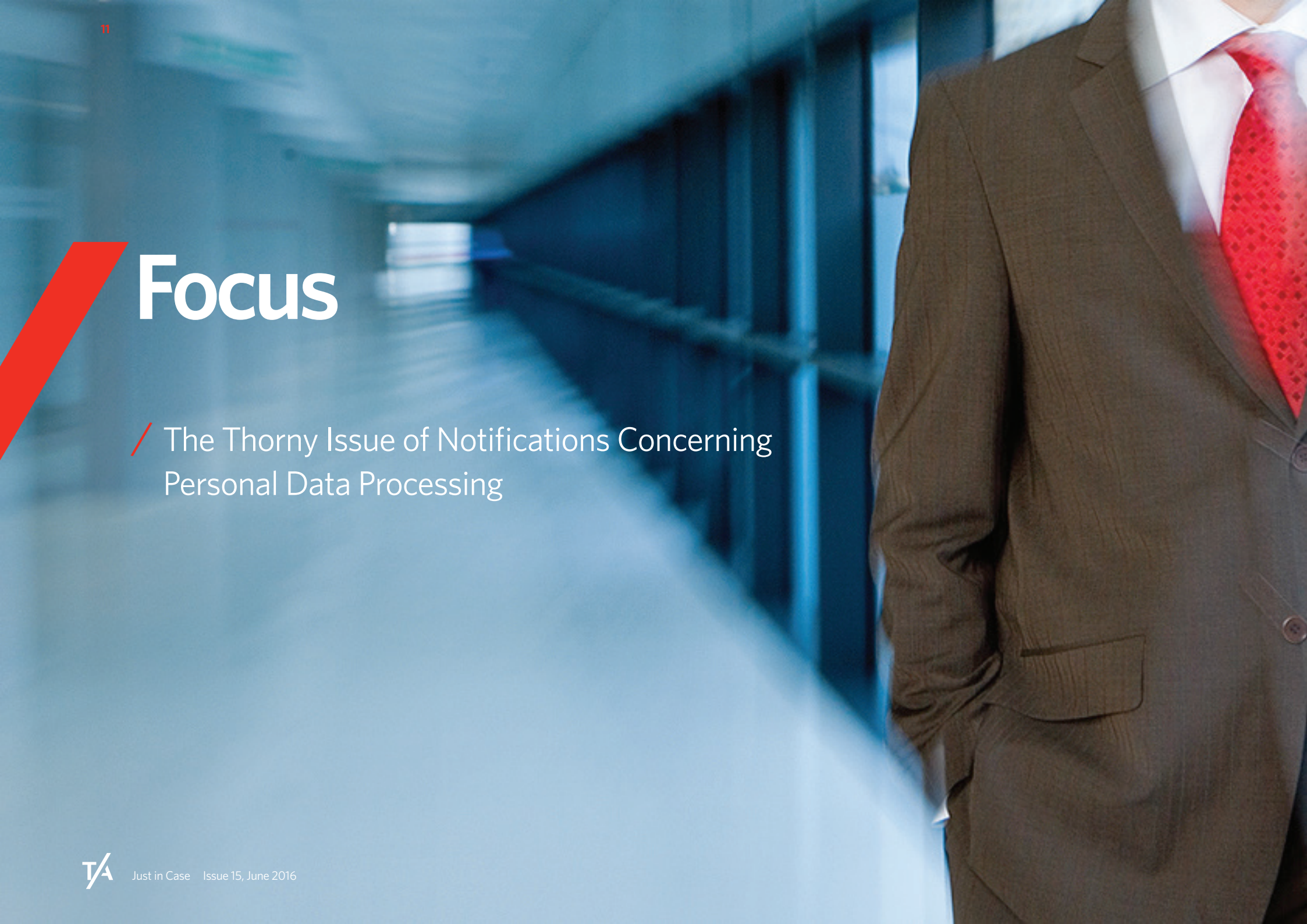
- **Preventing the access to data requested directly by foreign government bodies** - providers should be aware that generally speaking, there are no "blocking statutes" in Romania (imposing criminal or civil penalties on in-country persons complying with orders/requests issued by foreign authorities), which may be used to prevent the disclosure of data following a request for production of data made directly by a foreign government authority, without first going through the Romanian government. However, in certain cases, the requirements under the data protection law may hinder the provision of such data to a foreign government body. For example, the transfer of personal data to unsafe countries is allowed only under certain conditions (e.g. data subject's consent, or based on adequate contractual clauses and subject to approval by the Romanian data protection authority). Therefore, any direct request from foreign authorities for the production of data should be carefully assessed on a case-by-case basis, so as to avoid any potential sanctions under the data protection legislation.

Sergiu Crețu,
Senior Associate
sergiu.cretu@tuca.ro

Roxana Pană,
Senior Associate
roxana.pana@tuca.ro

Focus

The Thorny Issue of Notifications Concerning Personal Data Processing



The Thorny Issue of Notifications Concerning Personal Data Processing

Decision No. 200/2015 of the National Supervisory Authority for Personal Data Processing (ANSPDCP) ("Decision 200/2015") regulates the issue of notifications concerning personal data processing.

Essentially, according to Article 1 of Decision 200/2015, except in certain cases of processing that are expressly and exhaustively detailed in the decision, it is unnecessary to notify ANPSDCP when processing personal data. Moreover, in accordance with Article 2 of the Decision 200/2015, personal data transfer to countries outside the European Union or the European Economic Area (EEA), and to countries that are not recognised by the European Commission as providing adequate protection, on the basis of a decision, must be notified[1] to or, as the case may be, authorised[2] by ANSPDCP.

As arising from the preamble to Decision 200/2015, it was targeted at avoiding "inadequate" administrative formalities (which is a politically correct way of saying "useless"), by reference to the nature of the processing, and the actual risks that it entails for the data subjects.

Surely, releasing the controllers from the obligation to notify all personal data processing operations is by all means welcome and well-timed. However, as we shall be discussing below, the manner of regulating such an exemption is debatable as regards its compliance with the provisions of Law No. 677/2001 and of the relevant European regulations.

In accordance with Article 22(1) of Law No. 677/2001, data controllers are obliged to notify ANSPDCP in relation to any such operation they are carrying out. Nonetheless, while Article 22(2) lists a series of processing operations that need not be notified to ANSPDCP, paragraph (9) of the same article provides that the supervisory authority may establish other situations where the notification is not required (other than those under paragraph (2)).>

1. If the personal data transfer is based on the consent of the data subject, or in any of the other cases allowing for such transfer, provided at Article 30 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 ("Law No. 677/2001").

2. If the controller provides sufficient guarantees to ensure the protection of the fundamental individual rights, in accordance with Article 29(4) of Law No. 677/2001.

On that account, as a rule, personal data processing operations need to be notified to ANSPDCP in accordance with Law No. 677/2001; by way of exception, notification is not required for the processing provided at Article 22(2) of Law No. 677/2001, and for other processing operations expressly set out by ANSPDCP, on a case-by-case basis. Besides, the notification system set forth under Law No. 677/2001 was taken over from Directive 95/46/EC (Article 18).

With respect to the notification system for the processing of personal data, set forth by law No. 677/2001, Decision No. 200/2015 all but switched the rule with the exception. Thus, according to the Decision, the processing of personal data need not be notified to ANSPDCP, where the controllers are obliged to notify solely for the cases expressly and exhaustively provided in the decision. Nevertheless, according to the hierarchy of legislative acts, the secondary legislation issued by the central and local public administration authorities must comply with the laws enacted by the Parliament. A secondary piece of legislation (such as Decision No. 200/2015) cannot derogate from, supplement or amend a law (such as Law No. 677/2001).

Along the same lines, the compliance of the data processing notification system established under Decision No. 200 with the European provisions is also questionable. Directive 95/46/EC (Article 18) regulates in exhaustive terms two options meant to ensure the control of personal data processing, namely (a) notification-based control, and respectively (b) control through a specialised entity (the so-called data protection official).

Certain EU Member States (e.g. Germany, France, and Portugal) chose to implement the control through a data protection official, and therefore the obligation to notify does not apply at all. Since Romania opted for the notification-based control system (as per Article 22 of Law No. 677/2001), our opinion is that, in accordance with the current laws, this system could only be regulated in the manner envisaged by Directive 95/46/EC (Article 18). Or, Article 18 provides a notification system similar to the one regulated under Article 22 of Law No. 677/2001. Namely, in principle, the processing of personal data must be notified to the competent authority, who is however entitled to set forth exceptions from the obligation to notify, on a case-by-case basis.

To conclude, the change in paradigm as regards the notification of personal data processing could only be implemented by a legislative act with at least the same legal power as Law No. 677/2001 (i.e. by law or emergency ordinance, as the case may be). From this perspective, we could argue that Decision No. 200/2015 does not comply with Law No. 677/2001.

Regardless, we do not foresee any particular consequences on a practical level, from the perspective of data controllers. As a matter of principle, data controllers would not be interested in challenging the legality of the provisions under Decision No. 200/2015 (setting forth a more permissive notification system). Besides, it is highly unlikely that ANSPDCP should sanction a personal data controller for failing to notify according to the provisions of Law No. 6777/2001 (although such processing did not require notification, in accordance with Decision No. 200/2015).

Conversely, the notification mechanism set forth by Decision 200/2015 might prove to be more vulnerable and more likely to create loopholes in the main objective of the relevant legislation, namely protecting the rights of data subjects. For instance, although significantly risky, certain personal data processing operations which were not provided under Decision No. 200/2015 could go below the radar of ANSPDCP.

Likewise, it is possible that future processing operations might be carried out, that could entail significant risks for the data subjects' private life (for instance, processing performed by particularly intrusive means, further to the accelerated development of technology), which were not covered under Decision 200/2015. Or, until the express regulation thereof, such data processing (susceptible of posing particular risks for the data subjects' interests) would not be subject to the obligation to notify (although, according to the relevant regulations, data processing likely to raise particular risks should be notified to ANSPDCP).

However, we would point out that Decision 200/2015, as it currently stands, shall be applicable until the entry into force of the European Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (foreseen to enter into force in 2018). This EU Regulation shall fully remove the obligation to notify, setting forth other alternative mechanisms to ensure the protection of data subjects. But let us discuss these alternatives on another occasion.

Ciprian Timofte,
Managing Associate
ciprian.timofte@tuca.ro

News and Views

The Watchful Eye

The Watchful Eye

As part of our value-added client service programme, Țuca Zbârcea & Asociații regularly host bespoke events for the firm's clients and other interested parties.

Our public speaking events have always aimed at creating a platform for debate, as well as trying to find solutions to legal issues that weigh on our clients' minds. Drawing on their experience, our lawyers and consultants are genuinely interested in interacting with broad audiences in order to convene people from divergent economic sectors so as to reach desirable answers for the debated subjects.

Our latest seminar, "Monitoring vs. Privacy of the Employees at the Workplace. Current Legal Dilemmas and Practical Solutions", took place on 31 May at the Cesianu-Racoviță Palace (the Artmark Galleries), and it proved to serve its purpose.

As a fair balance between the employer's interests and the employee's right to privacy is an extremely delicate issue, that might often give rise to numerous predicaments and controversies, we found it necessary for a discussion to be carried out in this regard. Moreover, recent enactments, such as the EU Regulation concerning data processing (i.e., the ECHR judgement in the Bărbulescu vs. Romania case), provided for a good occasion to comment on the impact of the latest case-laws in this matter.

Along with the Țuca Zbârcea & Asociații team (Bogdan Halcu, Managing Associate; Ciprian Timofte, Managing Associate; and Sergiu Crețu, Senior Associate) specialising in data protection, speakers and representatives of the National Supervisory Authority for Personal Data Processing (ANSPDCP) took lead in the presentation and the ensuing discussions.

Since its announcement, the event has quickly gained people's interest and thus approximately 50 legal advisors, Human Resources managers, directors of internal audit (compliance) and specialists in the legal, administrative and even IT fields have joined our speakers, all interested in strengthening their knowledge on data privacy in relation to monitoring employees. The debate was highly appreciated, as the relevant news in the field were combined with case studies at hand. Not only did this discussion bring an insightful overview upon recently enacted regulations, but it also raised a well-based round of Q&A that helped put people's mind at ease when applying the knowledge to their specific work situation.

Most of the discussion was focused on matters concerning principles and general rules for monitoring employees, such as consent to monitoring and>

the need to provide this consent, internet and e-mail monitoring, video and audio monitoring at the workplace, GPS, and electronic access systems, from a legal and moral perspective.

With all the flow of information and emergence of social media networks, employers tend to become more and more reluctant to allow this kind of interaction at the workplace, and thus the dialogue invariably digressed to the Facebook issue. Another highly debated subject, that stemmed from the social media discussion, was that of the "Blanket Ban", and whether or not employers are allowed to completely prohibit employees from using the Internet for personal purposes, or from connecting personal devices to internet sources from work.

Further technological developments that may challenge the principles of data privacy are expected in the future, therefore the issue of monitoring employees will most likely remain an open question. However, our team at Țuca Zbârcea & Asociații is continuously working on keeping up with the legal framework, so as to be ready to address your issues on the matter. Our approach combines client work with public speaking engagements, editorial contributions and the creation of an online tool to raise awareness of the risks of personal data processing, while also keeping an eye on new developments in the relevant national and European regulations. As such, in November 2014, Țuca Zbârcea & Asociații marked a first in Romania by launching a dedicated web-based platform - **dataprivacyblog.tuca.ro**. Please feel free to visit our website should you be interested in knowing the rights and obligations regarding respect for private life, generically included in the concept of "privacy", or learning more about how the abundant recent IT&C services and solutions work, as well as about the advantages and disadvantages of various technologies, but also the risks in relation to the use, storage and publication of personal data on the world wide web.

Alina Pintică
Chief Marketing and Communications Officer
alina.pintica@tuca.ro

Ana Maria Pandelea
PR & Marketing Assistant

/ **The materials included herein are prepared for the general information of our clients and other interested persons. They are not and should not be regarded as legal advice.**

Victoriei Square
4–8 Nicolae Titulescu Ave.
America House, West Wing, 8th Floor
Sector 1, 011 141, Bucharest

Ⓣ +40 (21) 204 8890
Ⓕ +40 (21) 204 8899
Ⓔ office@tuca.ro
Ⓦ www.tuca.ro