Balázs Fazekas

Data Protection from a Practical Perspective

1. Incomplete harmonization of community law?

When foreign lawyers or clients seek advice regarding the Hungarian regulatory environment of data protection, and would like to assess whether Hungarian data protection law poses any specific issues they need to observe when doing business in Hungary, the evident advice is that there is nothing to be afraid of, as Hungarian data protection laws are, as a result of the accession of Hungary to the EU, fully harmonized with the relevant EU laws, which are more or less familiar to most of the clients.

Although the above is true in general, it is time to stop for a moment and think it over again. Is it true that Hungarian data protection law (Act LXIII of 1992 on protection of personal data and transparency of public data, the "DPA") fully transposes the relevant EU directive, i.e., the 95/46/EC Directive (the "Directive")? Are there legal institutions which are missing from the Hungarian legal system? Are there specific Hungarian "inventions" in our legal system which are not compatible with community law?

First I propose to go back to the basics and explore the *definitions*. Under community law, the distinction between "data controller" and "data processor" is evident. The decisive element is that data "controlling" involves a decision on the use of the personal data, while "processing" describes all the activities what are physically or technically possible with the data. Although the definitions in the DPA seem to be in line with the Directive, in Hungarian practice processing is often confused with a computerized technical process.

Another are of concern are the *exemptions from the general rules*. Under Article 3 of the DPA, the legal title required for lawful controlling of personal data is either the consent of the data subject or a specific authorization of law. (Such authorizations are provided by the acts on electronic communications, police, etc.) On the other hand, Article 7 of the Directive provides other titles (see paragraphs (a) to (f) of Article 7 for details). Apparently, Article 3 of the DPA is a misinterpretation of the corresponding rules of the Directive. In practical life, the inability to base a data controlling on the additional titles (exemptions) causes significant practical problems for companies which would like to act prudently and legally, but whose room to maneuver is very much restricted by the rigidity of the DPA.

The third, and (at least in our practice) the most frequent problem is the issues of consents and the provision of information for purposes of obtaining the consent. General principle of data protection law is that all data controlling requires (if not authorized by law) the consent of the data subject. Before asking for the consent, the data subject should be put in a position so that he/she is able to assess the consequences of his/her consent, i.e., assess whether the proposed controlling poses any risks to his/her privacy or otherwise. To this end, the data subject should be provided sufficient information on the nature and circumstances of the data controlling, such as the purpose and duration of the data controlling. The DPA precisely sets forth the scope of information to be provided in its Article 6(2). In the event the data is transferred to a third party, similar information on the third party should be provided before asking for the consent.

In Hungary, no real best practice has been developed as to the depth and level of information to be provided. Companies can (and should) rely on the above general rules and also the relevant notices and recommendations of the data protection commissioner. However, the general rule implies, and this is further supported by the data protection commissioner, that the information to be provided should be most specific, and should include all the details of the data controlling, and in the event of a data transfer, the exact identity of the recipient (including full (company) name, address, etc.).

On the other hand, the Directive seem to provide a more relaxed regime for information provision: Article 10(c) suggests that it is also sufficient when the information provided relates to the "categories" of recipients of personal data.

This ambiguity causes significant practical problems for companies wishing to act legally. Let's assume that a company which regularly collects personal data from its customers, clients, etc. outsources the processing of such data to a third party data processing entity. Let's also assume that the company, in order to be fully compliant with Hungarian law, precisely notified the data subjects about the exact identity of the data processing entity. What is the right practice when the data controlling company is not satisfied with the data processor and wishes to replace it with another entity? Although this is totally reasonable from a business perspective, the company may not be able to do this without enormous efforts, as it needs to notify all its clients, consumers, contacts, etc. about the identity of the new data processor and ask for a new consent for the processing by this new entity. If the company has links to thousands (or even millions) of data subjects, the above practice is more than unreasonable.

In the practice, the companies need to find the right balance between flexibility (provision of a reasonable amount of information) and being conservative, i.e., the provision of maximum information on the data controlling and processing. The position of the data protection commissioner suggests that a conservative view should be taken. It is very likely that a court would take the position of the data protection commissioner very seriously in a court procedure, even though the courts are not bound by such position. Thus, the companies are recommended to take a rather conservative view. Unfortunately the right depth of information to be provided has never been tested in a court litigation, and a concept of "reasonable amount" of information (let alone a sophisticated test to assess whether the information provided by a company has been sufficient) has not been developed by the courts.

The author is associate at Réczicza White&Case, Budapest

2. Personal data, private information (privacy), trade secrets

Without elaborating in detail on the definition of personal data and private or trade secrets, it is generally true that personal data is every data through which a private individual can be identified, while there are also information which are not personal data in the strict sense but which still belong to the private sphere of a private individual (personal secrets or private information) or a company (trade secrets). The two types of information falls under somewhat different (although not at all independent) legal protection regimes (i.e., specific data protection laws and protection of personal rights including privacy under the civil law).

In practical life, it is very common that a single piece of information constitutes both a personal data and private information, or at least some portions of the information (incorporated e.g. in a company memorandum or an email) are personal data (names, addresses, telephone numbers) while other parts are rather private information only (contents of the conversation).

We are all aware that monitoring of employees by the employers, e.g. by means of tracking internet usage or reading the emails of employees, is becoming widespread. Although typically such monitoring is often viewed by the employees as offensive, we should be clear that employer's have legitimate interest they wish to protect by means of the monitoring, and they have the right to do that. Monitoring may be required also for purposes of an audit or investigation (e.g., to comply with stock exchange rules) or in order to respond to request of authorities. It is very positive that the data protection commissioner, in pace with the development of such monitoring techniques, issued recommendations on the proper interpretation and practical implementation of data protection rules in connection with monitoring, and warned companies to fully observe such recommendations.

Such recommendations, however, deal primarily with personal data, and are not always possible to apply them easily to other private information or trade secrets a company may learn in the course of the monitoring. In our view, a company will be considered as acting prudently when it complies both with data protection rules and other privacy rules at the same time. Therefore it is necessary for the companies to understand that, when implementing monitoring measures, a proper legal solution should be implemented for protection of private information as well. E.g., companies recently often include in their general terms of employment that computers and internet are provided for the employees for business purposes only, they cannot be used for private purposes, and the company has the right to access all data stored on company computers or included in emails or other Internet communication. However, the employees may still say that, on the hard drive of the computers and in the emails, there are (a) personal data which do not belong to them, so their consent is not sufficient for the controlling of such third party data (e.g., emails received from private friends, with names, telephone cumbers, etc., or even business emails with personal data, unless the sender was aware of the circumstance of the controlling of such personal data by the recipient, in which case an implied consent can be considered as given), or (b) the email or documents contain private secrets which are not personal data in the strict sense but in relation to which the employee, or even another interested third party (if that is the case) may want to reserve his/her rights.

Therefore in my view it is necessary that consent granted by the data subject to the controlling of personal data extends to the access of any further private information. The consequences of not being prudent in developing and implementing a proper consent regime may be harsh if the information accessed by the company contains sensitive information without the owner of the information made aware of the monitoring.

3. Data transfers – intra-group transfers

In business life, it is very common that a multinational company, comprising of local businesses in various countries, shares information among its affiliates. It is also typical that certain central functions (e.g., human resources administration, payroll functions, benefits administration, client complaints) are handled by one designated affiliate in the group, typically the head office. It is also often the case that the local arms of the multinational company are located on different continents and in countries with different legal regimes, including data protection regimes. A relatively new phenomenon in Hungary is the appearance of "shared services centers", meaning an entity to which certain functions, very often administrative functions of the group are outsourced in its entirety. The operation of such shared services centers usually involves the transfer of various personal data (employees, customers, suppliers, etc.) to an from the center on a mass scale.

Hungarian law does not consider groups as a single entity, and transfer of personal data within the group requires observation of the same rules as in the event of transfers among independent third parties. (Of course, development and practical implementation of a uniform group level data protection regime is less difficult within a group under common control.) Some jurisdictions recognize groups and provide relaxed data protection rules for groups. The purposes of data protection laws is to protect the rights and privacy of private individuals. It is fair to say that normally, in the event of an intra-group transfer of personal data, the risks associated with the possible breach of rights and privacy of private individuals are lower, or at least it is relatively easy to mitigate such risks. In the event of intra-group transfers, the aim of the transfer is evident (such as, payroll), the flow of data is transparent (group entities), the security measures can be made uniform (global IT systems), all mitigating the data protection risks. Also, it is absolutely possible, and recommended, that a global data protection and privacy policy is put in place. If personal data of employees are concerned, it should also be noted that there are existing and well-established interfaces between the employees and the employers which may be used also for obtaining consent or seeking remedies.

4. Data transfers to foreign authorities

In a our global world, from time to time Hungarian and foreign authorities need to share information they have on companies, including for purposes of provision of legal assistance by an authority to another authority. The cooperating authorities are often not certain as to how, under what circumstance, under what procedure, and what scope of personal data may be transferred between them for purposes of legal assistance.

A practical example: The SEC, the U.S. Securities and Exchange Commission has regulatory powers over certain Hungarian companies which are listed on the New York Stock Exchange. Of course, these Hungarian companies are subject also to Hungarian law, and so long they are listed on the Budapest Stock Exchange, are also subject to the regulatory powers of the PSZAF, the Hungarian Financial Supervisory Authority. If the SEC believes that there is a criminal act committed within the company (and US securities law has become rather strict recently), it will turn

to the Hungarian PSZAF for information on the grounds of international agreements on legal assistance in criminal matters. However, as a general rule, PSZAF cannot provide the required information on such basis if the alleged crime is not a crime under Hungarian law. The PSZAF would rather like to rely on the international cooperation agreements among securities commissions, which may not be applied by the SEC in the given situation. Apparently, there may be different regimes in place governing data transfers between authorities located in various countries, and it is not always clear what legal regime should be used in a given situation.

5. Data transfers – chain of transfers

In a global world, a global company usually maintains office around the world. Let's imagine a global company with offices in Budapest, London, New York and Singapore. Let's also imagine that the London office is responsible for collecting certain personal data (e.g., of employees, clients, etc.) in Europe from the European offices, than it aggregates such data and forwards it to New York and Singapore (e.g., for billing, escalation of client complaints, payroll, etc.). A number of questions arise: Is the London office a data controller or a data processor? Does the Budapest office, prior to the transfer, need to verify if New York is registered as falling under the "Safe Harbor" rules, providing a sufficient level of protection? What about Singapore? Does the Budapest office need to be a party to a data processing agreement under the EC standard contractual clauses for purposes of the data transfer with London, New York or Singapore? I do not intend to answer these questions now; I just tried to illustrate the range and nature of data protection issues a global world raises.

6. Rights of data subjects to enforce agreement

The EU developed standard contractual clauses (SCC) to govern the transfer of personal data for purposes of data controlling and data processing by an entity located in another (non-EEA) country. One of the most important aims of such SCC is to ensure that, by the inclusion of its terms in a data transfer agreement to be concluded between the transferor and the recipient, appropriate remedies are made available to data subjects affected by the transfer.

It is important to note that in some countries the data transfer agreement needs to be registered by, or at least notified to, the data protection commissioner (or the similar relevant office). The question is whether data subjects are able to exercise their rights under such agreement even in the absence of such registration/notification. Arguably, even if the agreement is not registered/notified, the data subjects are authorized to exercise the remedies, otherwise the purposes of the agreement (i.e., to provide remedies to the data subjects) cannot be achieved.

Also, a question is whether the data transfer agreement needs to be disclosed to, or possibly consented by, the data subjects in order to provide remedies to the data subjects. Arguably, the data subjects are authorized to exercise remedies even if they do not know about the existence of the agreement, or do not know the exact terms and conditions of the agreement. However, as a rule of thumb, relevant information on the remedies should be made available to the data subjects, otherwise the data subject will practically unable to exercise their rights. It is preferred that an extract of the agreement itself (if not the entire agreement) is provided to the data subjects for information purposes.

7. Law office as data controller

Under the Act on Attorneys (Act XI of 1998), the attorney (and the law office) is de facto a data controller, as it needs to establish a relationship with the client which inevitably involves the collected of facts, information, data, including personal data. Here the problems lies within the co-existence of two regimes governing data controlling by attorneys, i.e., the regime provided by the Act on Attorneys and the DPA. An examination of the two regimes reveals that there are certain discrepancies between the two regimes:

The Attorneys Act recognizes special operational forms, such as the association of offices. On the other hand, the DPA does not provide special rules for such an association. Although a transfer of data among the associated offices, including if the offices are in multiple countries, is arguable permitted by the Attorneys Act, such transfer is viewed as a transfer to a third party under the DPA. As a consequence, if such transfer involves transfer to a recipient to another jurisdiction, the level of protection provided in such other jurisdiction should also be judged (unless the recipient is within the EEA). A practical issue is whether and how, in case of transfer among law offices, the level of protection provided by the legal regimes governing secrecy requirements posed on attorneys should also be taken into account, on top of the "general" data protection regime in the relevant jurisdiction.

Another issue to be explored is the difference between treatment of client data and other third party data by law offices. In the daily practice, a law office normally collects and processes various personal data, including (a) client data, primarily for administration and billing purposes, and (b) other third party data, such as data of the counter-party in a litigation, contact lists with contact details of people delegated by various entities working on a transaction (so-called "working party lists"), contact details of persons to be inserted into agreements for notification purposes, and various other data learned in a due diligence review procedure. It is fair to say that client data and those third party data which were provided by the respective party or person voluntarily (e.g., a working party list) do not raise legal issues, as by providing the data, and in awareness of the purpose and other circumstances of the use of the data, the respective data subjects grant an implied consent to the controlling of their data by the law office. However, controlling of those data which are gathered without the data subject knowing about the data controlling activity (such as learned in a due diligence procedure) arguably raise legal issues. Nevertheless, all such data will still be considered as attorney secrets and cannot be disseminated to third parties.

The general legal position is that the Attorneys Act provides sufficient title for the data controlling for the law office or the actual lawyer having access to the above data. However, in daily life, such information often needs to be shared among other lawyers or law offices, and even with other entities. It is somewhat unclear to what extent such transfer is permitted or would require additional measures to ensure legality. (It depends on various factors, but most importantly, whether an implied consent can be considered as given in the actual situation.) In the practice, to be on the safe side, the parties make almost all information transfers (including transfer of personal data, business secrets, etc.) subject to the signing of a confidentiality agreement by the recipient party. However, such confidentiality agreements usually do not extend to special data protection considerations and may not always be sufficient for data protection purposes.

8. Consent in online environment

Data protection in online environment raises additional questions. One of the issue areas

is whether and how a consent to a data controlling may be obtained in an online environment.

Under Hungarian civil law, minors under 18 have no full capacity to make legal representations and statements concerning their personal rights. If an online service is open to minors, and in particular if the online service is specifically targeted to minors (such as websites of children and cartoon television channels, websites of online games, etc.), the circumstances of obtaining the consent should be designed very carefully. If the user is a minor, his/her consent in itself is not sufficient but the consent of the parent should also be collected. As the operator of the online service cannot verify the age of the user with a total certainty, the operator of the service should be able at least to demonstrate that it made its best efforts to ensure that the consent is properly obtained and the consent of the parent is collected.

As a practical solution, it is recommended that whenever user data is collected, the site request for a confirmation of the age of the user. When the user is a minor, an additional consent should be obtained, either by sending out a specific email to a given email address, or by specifically stipulating that such additional consent is given by the parent. Of course, the operator of the website will have no bullet-proof tools to verify if such additional consent is provided really by the parents (it would require unreasonable efforts or unfeasible measures), but at least the best effort can be proven. We note that online financial services use very sophisticated identification methods, however, this level of scrutiny may not be justified in the event of general online services.

Another focus area of data controlling in an online environment is the data protection and privacy policy of the online service. It is fair to say that as soon as a service is made available in Hungary or targeted to Hungarian users, such service will fall under Hungarian data protection law and Hungarian data protection laws need to be observed. In our practice we often reveal that data protection and privacy policies of certain global services available also in Hungary are not fully compliant with Hungarian law (and here we mean not only data protection laws but other areas of law, such as online consumer protection laws). We believe that as soon as a company brings the business decision that it will offer a service Hungary, it should act prudently and duly localize its policies so that they comply with Hungarian law. (Another issue is how a Hungarian data subject could enforce its rights against a foreign online entity without a legal settlement in Hungary.)