



PRACTICAL LAW

MULTI-JURISDICTIONAL GUIDE 2012/13

DATA PROTECTION

The law and leading lawyers worldwide

Essential legal questions answered
in 30 key jurisdictions

Analysis of critical
legal issues





Hungary

János Tamás Varga and Zoltán Tarján
VJT & Partners Law Firm

www.practicallaw.com/3-502-4056

REGULATION

Legislation

1. What national laws regulate the collection and use of personal data?

General laws

In 2011, the Hungarian Parliament adopted a new act on data protection, Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information (DPA), which came into effect on 1 January 2012 and implements Directive 95/46/EC on data protection (Data Protection Directive). The DPA aims to guarantee the rights of individuals to exercise control over their privacy and to have access to data of public interest and public data on the grounds of public interest. The DPA is regarded as background legislation for specific statutes regulating the collection and processing of personal data.

Sectoral laws

In addition to the DPA, the following statutes are particularly relevant for data protection purposes:

- **Act XLVII of 1997 on Processing and Protection of Medical and Other Related Personal Data (Medical Data Act).** This regulates the conditions and purposes of the processing of sensitive data concerning an individual's state of health and related personal data.
- **Act LXVI of 1992 on Personal Data and Address Records of Citizens.** This provides detailed rules on the use of records containing individuals' personal data, including their address.
- **Act C of 2003 on Electronic Communications (Electronic Communications Act).** This regulates the processing of subscribers' personal data by communication service providers, including the obligation to retain data.
- **Act CXIX of 1995 on Processing of Name and Address Data for Research and Direct Marketing Purposes.** This contains regulations on the processing of name and address data for the purposes of research and paper-based direct marketing.
- **Act XXII of 1992 on the Labour Code.** This regulates employers' processing of employees' personal data. This is due to be replaced by Act I of 2012 on the Labour Code which will come into effect on 1 July 2012.
- **Act LX of 2003 on Insurance Companies and Insurance Activity (Insurance Act).** This provides detailed rules on the processing of clients' personal data that qualifies as an insurance secret.

- **Act CXII of 1996 on Credit Institutions and Financial Undertakings (Credit Institutions Act).** This regulates the processing of clients' personal data that qualifies as a bank secret.
- **Act XLVIII of 2008 on the basic conditions of and certain restrictions on business advertising activity (Advertising Act).** This regulates the processing of personal data for direct marketing purposes.
- **Act CVIII of 2001 on electronic commercial services and services related to information society (Electronic Commerce Act).** This provides rules on sending unsolicited electronic commercial communications.

Scope of legislation

2. To whom do the laws apply?

The DPA applies to individuals or legal persons that qualify as "data controllers" or "technical data processors".

A data controller is any individual or legal person or any organisation without legal personality that (DPA):

- Determines the purpose of data processing (alone or together with others).
- Makes decisions on data processing (including concerning the means of processing).
- Implements these decisions or has them implemented by a technical data processor.

A technical data processor is any individual or legal person or organisation without legal personality that on the basis of a contract concluded with the data controller (including conclusion of a contract on the basis of legislation) performs technical processing of data.

Whilst a data controller determines the purpose of data processing and makes decisions on data processing, a technical data processor can only perform technical tasks related to data processing operations, and technically process personal data on the basis of the data controller's instructions. The technical data processor is not entitled to make any decision on the merits concerning data processing.

The DPA also applies to "data subjects". A data subject is any specified individual who is, or can be, directly or indirectly identified by any personal data (DPA).



3. What data is regulated?

The DPA defines “personal data” as any data relating to a data subject, as well as any conclusion in relation to the data subject, which can be inferred from those data. During data processing, data remains personal data, provided its relation to the data subject can be restored (that is, if the data controller has the technical means that are necessary for the restoration). Personal data includes especially:

- The data subject's name.
- Any identification code.
- One or more pieces of information specific to the data subject's physical, physiological, mental, economic, cultural or social identity.

In practice personal data is interpreted broadly. As a result, the term personal data covers (among others):

- Biometric information.
- Sound recordings.
- E-mail addresses.
- IP addresses identifying a computer.
- Websites.

In addition to personal data, the DPA defines the following specific categories of data:

- Sensitive personal data (*see Question 11*).
- Criminal personal data.
- Data of public interest.
- Public data on grounds of public interest.

4. What acts are regulated?

The DPA regulates “data processing”, which covers any operation or set of operations performed on data, irrespective of the applied procedure, such as:

- Collection.
- Obtaining.
- Recording.
- Organisation.
- Storage.
- Modification.
- Use.
- Query.
- Transfer.
- Disclosure.
- Reconciliation.
- Combination.
- Blocking.

- Deletion.
- Destruction.
- Prevention of further use of the data.
- Photographing, sound or image recording.
- Recording of physical characteristics which could be used for the identification of an individual (such as fingerprints and palm prints, DNA samples and iris images).

Contrary to the Data Protection Directive, the DPA defines the term of “technical data processing” as the performance of technical tasks related to data processing operations, regardless of the methods or means applied or of the place of application, provided that the technical tasks are performed on the data. The distinction between data processing and technical data processing can be made on the basis of the definitions of data controller and technical data processor (*see Question 2*).

The DPA applies to wholly or partially automatic and manual data processing as well as technical data processing.

5. What is the jurisdictional scope of the rules?

The DPA applies to all data processing and technical data processing performed in the territory of Hungary that either relates to the data of individuals, or to data of public interest or public data on grounds of public interest.

The DPA applies if a data controller performing data processing outside the territory of the EU:

- Entrusts (for the purpose of technical data processing) a technical data processor having its headquarters, premises or residence in the territory of Hungary.
- Uses equipment that is located in the territory of Hungary, except when the equipment is solely used for the transit of data through the territory of the EU.

These data controllers must appoint a representative in the territory of Hungary.

6. What are the main exemptions (if any)?

The DPA does not apply to data processing that solely serves the personal purposes of an individual.

Notification

7. Is notification or registration required before processing data?

Before commencing data processing activities (except for mandatory data processing) the data controller must notify the National Data Protection and Freedom of Information Authority (the Authority), where applicable, of the:

- Purpose of data processing.
- Legal basis of data processing.
- Scope of data subjects.

- Description of data relating to data subjects.
- Source of data.
- Duration of data processing.
- Type of transferred data.
- Recipient of the transferred data.
- Legal basis of the transfer.
- Name and address of the headquarters of the data controller and the technical data processor, the place of data processing and technical data processing, and the activity of the technical data processor.
- Technical data processing method applied.
- Name and the contact information of the internal data protection officer.

The Authority must be notified of any change in the information registered within eight days.

The DPA specifies exemptions from the notification obligations, such as data processing:

- Involving the data of persons having an employment, membership, kindergarten, student, college or customer relationship (except for customers of financial organisations, public utilities services providers and electronic communication services providers) with the data controller.
- According to the internal rules of church or religious communities.
- Involving data relating to the diseases or state of health of persons receiving medical care, for purposes of medical treatment or preservation of health or for social insurance claims.
- Involving personal data recorded for the purpose of financial and other social support of the data subject.
- Involving data relating to the administrative, prosecution and court proceedings of data subjects affected by these procedures or relating to imprisonment.
- Involving data processed for the purpose of official statistics, provided the connection between the data subjects and the data cannot be restored.
- Containing data belonging to a media content provider, which serve solely its own information activity.
- Serving the purpose of scientific research, if the data are not published.
- Relating to archived documents.

Notification can be performed by completing a notification form in hard copy. The DPA does not specify the language in which the notification must be made to the Authority, but the notification form that can be downloaded from the Authority's website is available only in Hungarian. On registration, the data controller receives a registration number, which must be used for every transfer, disclosure and supply of the personal data.

Generally, the Authority must register the data processing within eight days from receipt of the notification provided that the notification

contains all of the necessary information. If the Authority fails to register the data processing in time, the data controller can commence the data processing according to the notification.

In specific cases the Authority must register the data processing within 40 days from receipt of the notification (for example, if a financial institution or an electronic communication services provider processes additional client data or uses new technical data processing technology). In these cases the Authority registers the data processing on the condition that requirements of lawful data processing are met by the data controller.

Registration (except the notification of mandatory data processing) is subject to a registration fee to be specified in separate legislation.

The data protection register will be publicly accessible on the Authority's website (*see box, The regulatory authority*).

MAIN DATA PROTECTION RULES AND PRINCIPLES

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The DPA imposes the following main obligations on data controllers:

- **Compliance with data protection principles.** All personal data processing must comply with the following data protection principles:
 - data processing must be fair and lawful;
 - data is only processed for a specified purpose, to exercise a right or to perform an obligation. This purpose must be followed during all phases of data processing;
 - the data processing is indispensable and suitable to achieve its purpose;
 - data is processed only to the extent, and for the duration necessary, to achieve the purpose of data processing;
 - data is accurate, complete and, if it is necessary, kept up to date;
 - identification of data subjects is possible for no longer than it is required for the purpose for which the data is processed.
- **Obtaining consent.** The consent of the data subject must be obtained (*see Question 9*) except if the data processing is ordered by a statute or a local government decree for public interest reasons or the legal ground for data processing is ensured otherwise, based on the DPA (*see Question 10*).
- **Providing information.** The data controller must provide the data subjects with unambiguous and detailed information on all facts relating to the processing of his data (*see Question 12*).
- **Taking technical and organisational measures.** The data controller and (within the scope of its activities) the technical data processor are obliged to ensure the security



of personal data and to take all technical and organisational measures and establish the procedural rules necessary for compliance with the DPA and other rules relating to data protection and confidentiality (see *Question 15*).

- **Respecting the rights of the data subject.** The data controller must consider the data subject's requests made in accordance with the rights of the data subject under the DPA (see *Question 13*).
- **Notifying the Authority.** Before commencing its data processing activity, the data controller must notify the Authority of certain information to be registered (see *Question 7*).
- **Appointing an internal data protection officer and drawing up internal data protection regulation.** The following organisations, acting as either data controller or technical data processor, must appoint an internal data protection officer:
 - at bodies processing or technically processing national administrative, employment or criminal data files;
 - at financial organisations;
 - at electronic communication and public utility services providers.

Data controllers specified above and certain state and local government data controllers must adopt data protection and data security internal regulations.
- **Compliance with rules on data transfer outside the European Economic Area (EEA).** Data controllers must comply with rules on the transfer of personal data to a data controller or technical data processor pursuing data processing or technical data processing activities outside the EEA (see *Question 20*).

9. Is the consent of data subjects required before processing personal data?

The data subject's consent must be obtained, except if data processing is ordered by a statute or a local government decree for public interest reasons or the legal ground for data processing is ensured otherwise, based on the DPA (see *Question 10*).

Form and content of consent

The DPA requires that the data subject's consent must be:

- Given in advance.
- Freely given.
- Specific.
- Informed.
- Unambiguous.

To obtain the data subject's informed consent, the data controller must provide the data subject with unambiguous and detailed information on all facts relating to the processing of his personal data (see *Question 12*).

Generally, online consent is deemed sufficient, provided it is obtained in compliance with these requirements. Under the DPA, consent to data processing must be in writing in relation to sensitive

personal data (see *Question 11*). However, the data controller bears the burden of proof in relation to the lawfulness of data processing. Therefore, it is always advisable to record the data subject's consent in a retrievable format. Sector-specific regulations can set out more stringent conditions concerning the form of the consent.

Consent by minors

The consent of the minor's statutory representative must be obtained to the processing of the minor's personal data if the minor is under 14 (*Act IV of 1959, Civil Code*). Minors between the age of 14 and 16 can give their consent to the processing of their personal data, however, their statutory representative's approval must be obtained. Under the DPA, minors over the age of 16 can give their consent to the processing of their personal data without the consent or the subsequent approval of their statutory representative.

Implied or inferred consent

Consent from the data subject is deemed to be given (DPA):

- In a court procedure or administrative procedure initiated by the data subject with respect to personal data necessary for conducting the procedure.
- In another procedure initiated by the data subject with respect to personal data provided by the data subject.
- With respect to personal data provided by the data subject during his public appearance.

According to Act CXXXIII of 2005 on person and property protection and private investigation activity, persons pursuing property protection activity are entitled to operate surveillance cameras under specific rules. Notification regarding the operation of cameras must be visible. Consent can be given by implied conduct (for example, consent is deemed to be given if the individual enters the monitored area while aware of the notification).

10. If consent is not given, on what other grounds (if any) can processing be justified?

If consent is not given, the processing of personal data still complies with the DPA as follows:

- If a statute or a local government decree orders the data processing for public interest purposes.
- If obtaining the consent of the data subject is impossible or it would incur disproportionate cost, and processing of the personal data:
 - is necessary to fulfil the legal obligation of the data controller; or
 - is necessary for the legitimate interest of the data controller or a third party and the interest is proportional to the limitation of the right to the protection of personal data.
- If the data subject is not able to give his consent due to incapability or for another unavoidable reason, then his personal data can be processed to the extent necessary to protect his or another person's vital interest, or to prevent or avert imminent danger threatening a person's life, safety or possessions during the existence of obstacles to the consent.

- If the personal data were obtained on the basis of the data subject's consent, the data controller (unless statute provides otherwise) can process the personal data obtained without any further consent and even after the withdrawal of the data subject's consent:
 - for the purpose of performing his legal obligation;
 - for the purpose of the legitimate interest of the data controller or a third party if the interest is proportional to the limitation of the right to the protection of personal data.

Additional criteria apply to sensitive personal data (see *Question 11*).

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

Sensitive personal data is (DPA):

- Personal data concerning racial origin, national or ethnic minority origin, political opinion or party affiliation, religious or other ideological belief, membership in an interest group, or sexual life.
- Personal data concerning health, pathological addiction or criminal personal data. (Criminal personal data means any personal data generated during a criminal procedure or before that, in relation to crimes or criminal procedures by bodies entitled to carry out the criminal procedure, or to detect crimes, and at penal institutions, which can be associated with the data subject and personal data concerning criminal record.)

Sensitive personal data can be processed if one of the following conditions are satisfied:

- The data subject has given his written consent.
- It is necessary for:
 - the enforcement of an international treaty;
 - ordered by statute for the purpose of enforcing fundamental rights under the Hungarian Constitution;
 - for the purpose of national security, preventing or combating crimes or national defence (for sensitive personal data concerning racial origin, national or ethnic minority origin, political opinion or party affiliation, religious or other ideological belief, membership in an interest group or sexual life).
- It is ordered by statute for a public interest purpose (for sensitive personal data concerning health, pathological addiction or criminal personal data).
- Obtaining the consent of the data subject is impossible or it would incur disproportionate cost, and processing of the sensitive personal data:
 - is necessary for the purpose of fulfilling the legal obligation of the data controller; or
 - is necessary for the purpose of the legitimate interest of the data controller or a third party and the interest is proportional to the limitation of the right to the protection of personal data.

- The data subject is not able to give his consent due to incapability or for another unavoidable reason. In this case, data can be processed to the extent necessary to protect the data subject's or another person's vital interest, or to prevent or avert imminent danger threatening a person's life, safety or possessions during the existence of obstacles to the consent.
- The sensitive personal data were obtained on the basis of the data subject's consent, the data controller (unless statute provides otherwise) can process the sensitive personal data obtained:
 - to perform a legal obligation; or
 - for the legitimate interest of the data controller or a third party if the interest is proportional to the limitation of the right to the protection of personal data, without any further consent and even after the withdrawal of the consent by the data subject.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

The data controller must provide the data subject with unambiguous and detailed information on all facts relating to the processing of his personal data, in particular on the:

- Purposes and legal basis of the data processing.
- Persons authorised to carry out the data processing and the technical data processing.
- Duration of data processing.
- Person(s) authorised to have access to the data.
- Rights and remedies of the data subject in connection with the data processing.
- Fact that personal data are processed under section 6(5) of the DPA. That is if the personal data were obtained on the basis of the data subject's consent, the data controller (unless statute provides otherwise) can process the data obtained:
 - for the purpose of fulfilling his legal obligation; or
 - for the legitimate interest of the data controller or a third party if the interest is proportional to the limitation of the right to the protection of personal data, without any further consent and even after the withdrawal of the consent by the data subject, if applicable.
- Whether data processing is based on the consent of the data subject or whether it is mandatory.

13. What other specific rights are granted to data subjects?

Right to access

The data subject can request information on the processing of his personal data. The data controller must inform the data subject, on his request, of the:

- Data processed by the data controller or technically processed by the technical data processor.



- Sources of data processed or technically processed.
- Purpose, legal basis and duration of the data processing.
- Name, address and activity of the technical data processor in connection with data processing.
- Recipients of the personal data.
- Legal basis for transfer.

The data controller must provide the information in writing and in an easily comprehensible way within 30 days from receipt of the request. The provision of information in relation to the specific scope of data is free of charge once a year. Otherwise, the data subject requesting the information can be charged.

The data subject's right to access can be refused if:

- Statute restricts the data subject's right to access with a view to:
 - promoting the interests of the state's external and internal security, such as national defence, national security, crime prevention or criminal investigation;
 - promoting state or local governmental economic or financial interest;
 - promoting significant economic or financial interest of the EU;
 - preventing disciplinary and moral offences, or breaches of labour law or labour safety obligations;
 - protecting the rights of data subjects or of other people.
- The transmitting data controller informs the recipient data controller of specific processing restrictions in relation to processing of personal data under the framework of police and judicial co-operation in criminal matters.

Right to request rectification

The data subject can request the rectification of inaccurate personal data free of charge. If the accurate personal data are available to the data controller, then he must rectify them.

If the data controller refuses to rectify the inaccurate personal data, the data controller must inform the data subject in writing of the factual and legal reasons for the refusal within 30 days from receipt of the request and must also inform the data subject of the remedies available to him.

The data subject's right to rectification can be restricted by statute (*see above, Right to access*).

Right to request blocking

Instead of erasing, the data controller blocks the personal data if the data subject requests so, or where it can be assumed that the erasure would have an adverse effect on the legitimate interests of the data subject. Blocked personal data can be processed only while the purpose of data processing preventing the erasure exists. The blocking of personal data can be requested free of charge.

If the data controller refuses to block the personal data, the data controller must inform the data subject in writing of the factual and legal reasons for the refusal within 30 days from receipt of the request and must inform the data subject of the remedies available to him.

The data subject's right to blocking can be restricted by statute (*see above, Right to access*).

Right to object

The data subject can object to the processing of his personal data if:

- The processing (transfer) of personal data is necessary solely for performing the legal obligation of the data controller or enforcing the legitimate interest of the data controller, the data recipient or third party, except in the case of mandatory data processing.
- Personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research.
- Provided by statute.

The right to object can be exercised free-of-charge. The data controller must investigate the objection within 15 days from receipt of the objection. If the objection is justified, the data controller must discontinue the processing of personal data and block all personal data processed. If the data subject disagrees with the data controller's decision or the data controller misses the 15-day deadline, the data subject can initiate court proceedings within 30 days from receipt of the decision or the expiry of the deadline.

If the data recipient does not receive the data necessary for the enforcement of his right due to the objection of the data subject, the data recipient can initiate court proceedings within 15 days from the notification.

Right to refer the matter to court or the Authority

In case of violation of his rights or if the data subject disagrees with the data controller's decision regarding his objection, the data subject can initiate court proceedings against the data controller (*see Question 25*). As a general rule, court proceedings can be initiated within five years from the violation of the data subject's right (the general limitation period under the Civil Code).

Any individual can initiate an investigation before the Authority if any of the following has occurred:

- His rights have been violated in connection with the processing of his personal data, or having access to data of public interest or public data on grounds of public interest.
- There is an imminent danger of violation of his rights.

14. Do data subjects have a right to request the deletion of their data?

Except for mandatory data processing, the data subject can request the deletion of his personal data from the data controller, free-of-charge. Personal data must be deleted if:

- The processing of the personal data is unlawful.
- It is requested by the data subject (except for mandatory data processing).
- It is incomplete or inaccurate and cannot be corrected in a lawful way, provided deletion is not prohibited by statute.
- The purpose of processing has ceased to exist, or the legal time limit for the storage of data has expired (except if the storage device containing the personal data has to be archived under the law).
- This has been ordered by the court or the Authority.

If the data controller refuses to delete the personal data, the data controller must inform the data subject in writing of the factual and legal reasons for the refusal within 30 days from receipt of the request and must inform the data subject of the remedies available to him.

The data subject's right to deletion can be restricted by statute (see *Question 13, Right to access*).

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

The data controller (and within the scope of his activities the technical data processor) are obliged to ensure the security of personal data and to take all technical and organisational measures, and establish the procedural rules necessary for compliance with the DPA and other rules relating to data protection and confidentiality.

Personal data must be protected, especially against:

- Unauthorised:
 - access;
 - alteration;
 - transfer;
 - disclosure;
 - deletion or destruction.
- Accidental destruction and damage.
- Becoming inaccessible due to a change in the technique used for the data processing.

For the protection of data files processed electronically, it must be ensured by appropriate technical solutions that the data stored in the records cannot be directly connected and identified with the data subject, except where a statute allows it.

For automated technical data processing the data controller and technical data processor must take further measures to, among others, prevent unauthorised data inputs and to ensure the tracking down of data inputs and data transfers.

The data controller and technical data processor must consider technical developments relating to the application of measures serving the security of personal data. Out of the available data processing solutions, the one which ensures a higher level of protection for personal data must be chosen, except where it would cause disproportionate difficulty for the data controller.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is no general data security breach notification obligation. Electronic communications services providers must make a data security breach notification if there is a breach of the security of subscribers' personal data (*Electronic Communications Act*).

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

Technical data processors:

- Cannot make any decisions on the merit of data processing.
- Can only technically process the personal data as instructed by the data controller.
- Cannot technically process data for their own purpose.
- Must store and keep personal data according to the data controller's instructions.

The data controller is responsible for the lawfulness of the instructions given for technical data processors. In performing his tasks, the technical data processor cannot involve other technical data processors.

In addition, organisations with an interest in business activities using the personal data to be technically processed cannot be entrusted with technical data processing.

Contracts on technical data processing must be in writing.

ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

Storing data or gaining access to data stored on the electronic communications terminal equipment of the subscriber or user is only allowed on condition that the subscriber or user has given his consent, having been provided with clear and comprehensive information, including information on the purpose of the data processing (*Electronic Communications Act*).

For the type of consent required, see *Question 9*.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

Unless a statute provides otherwise, unsolicited electronic commercial communications can be sent to an individual only if that individual has given his prior, unambiguous and explicit consent (*Advertising Act*). The consent must include:

- The individual's name.
- Where the advertisement for which the consent is requested can only be communicated to persons of a certain age, the place and date of birth of the individual.
- The scope of personal data to be processed.
- An indication that the consent was given voluntarily based on appropriate information.

Consent can be withdrawn without restriction and reasoning, free of charge, at any time. The addressee of the unsolicited electronic commercial communications must be unambiguously



informed of the e-mail and postal address through which he can withdraw his consent. The request for consent must not contain commercial communications.

Sending a request for consent electronically qualifies as sending unsolicited electronic commercial communications, therefore, in practice, consent cannot be obtained through electronic means (*Electronic Commerce Act*).

Records of the personal data of individuals who have given their consent to receive unsolicited electronic commercial communications must be kept by the companies sending those communications.

INTERNATIONAL TRANSFER OF DATA

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The DPA does not set out specific restrictions on the transfer of personal data within the European Economic Area (EEA). Similarly, no specific restrictions are imposed on the transfer of personal data to Switzerland on the basis of a treaty with that country.

Personal data can be transferred to data controllers or technical data processors pursuing data processing or technical data processing activities outside the EEA (and Switzerland) if (DPA):

- The data subject has given his explicit consent.
- The conditions of data processing specified in *Question 10* are met and an adequate level of protection of the personal data in the third country is ensured during the processing or technical processing of the transferred data.

An adequate level of protection of personal data is ensured if (DPA):

- Mandatory legislation of the EU establishes it. In particular, the European Commission has recognised that certain third countries ensure an adequate level of protection. Approved destinations are:
 - Andorra;
 - Argentina;
 - Canada;
 - Faroe Islands;
 - Guernsey;
 - Isle of Man;
 - Israel (in relation to automated international transfers of personal data, or where they are not automated, they are subject to further automated processing in Israel);
 - Jersey;
 - Switzerland; and
 - US-based organisations that have signed up to the Safe Harbor privacy scheme.
- The parties use standard contractual clauses, which comply with the standard contractual clauses adopted by the European Commission.
- There is a treaty in force between the third country and Hungary safeguarding the rights and remedies of data

subjects as well as the independent supervision of data processing and technical data processing.

- Passenger name records of air passengers transferred to the US Bureau of Customs and Border Protection.
- EU-sourced passenger name record data transferred by air carriers to the Australian Customs Service.

An adequate level of protection of personal data is not required if:

- The data subject has given his explicit consent.
- Personal data are transferred for the purpose of implementing an international legal assistance treaty or a treaty on the avoidance of double taxation.

Neither the DPA nor its official reasoning regulate or refer to the use of binding corporate rules (BCRs). It is unclear whether the Authority will consider BCRs as a means of ensuring adequate levels of protection of personal data. Even if BCRs are considered adequate, it must be noted that BCRs in themselves do not serve as a proper legal basis for the transfer of personal data to third countries within a company group as additional conditions must be met (*see above*).

Data transfer agreements

21. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

The use of standard contractual clauses adopted by the European Commission is deemed to ensure an adequate level of protection (*see Question 20*).

The Authority has not approved a standard-form data transfer agreement.

22. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Data transfer agreements ensuring an adequate level of protection do not serve as a proper legal basis for transfer of personal data to any third country as additional requirements must be met (*see Question 20*). However, if the data subject has provided his explicit consent to the data transfer, there is no requirement for an adequate level of protection.

23. Does the relevant national regulator need to approve the data transfer agreement?

Data transfer agreements do not require the Authority's approval.

ENFORCEMENT AND SANCTIONS

24. What are the enforcement powers of the national regulator?

The Authority supervises and facilitates the enforcement of the rights to protection of personal data, and to access to data of public interest and to public data on grounds of public interest.

Among other things, the Authority conducts investigations on request. During an investigation the Authority is entitled to:

- Inspect all relevant documents.
- Request copies.
- Request information from the data controller or any organisation or person connected with the given case.
- Enter any premises where data are processed.

Where there are violations of law concerning processing of personal data or access to data of public interest and public data on grounds of public interest or imminent danger of it, the Authority calls on the data controller to remedy the violation of law, or to terminate the imminent danger. If the data controller fails to comply with this request concerning processing of personal data, the Authority can launch data protection administrative procedures. These procedures can also be launched without prior investigation if the violation of law requires immediate intervention.

The Authority must launch a data protection administrative procedure if there is a likelihood of unlawful data processing and the unlawful data processing:

- Affects a wide scope of persons.
- Affects sensitive personal data.
- May cause significant violation of interest or risk of damages.

In the course of a data protection administrative procedure the Authority can:

- Order the rectification of incorrect personal data.
- Order blocking, deletion or destruction of personal data processed unlawfully.
- Prohibit the unlawful processing or technical processing of personal data.
- Prohibit the transfer of personal data to foreign countries.
- Order that the data subject must be informed, if the data controller denied the information unlawfully.
- Impose a fine of between HUF100,000 to HUF10 million (as at 1 March 2011, US\$1 was about HUF215).
- Inform the public of its resolution and the identity of the data controller.

If the data controller fails to comply with the Authority's order concerning the violation of law regarding data of public interest or public data on grounds of public interest, the Authority can take the case to court.

If the Authority suspects that a crime has been committed, they are entitled to initiate a criminal procedure aimed at the authorised body.

25. What are the sanctions and remedies for non-compliance with data protection laws?

Criminal consequences

According to Act IV of 1978 on the Criminal Code "abuse of personal data" is the act of any person (for unlawful profit-making purposes or that causes a significant violation of interest) involving the:

THE REGULATORY AUTHORITY

National Data Protection and Freedom of Information Authority

W www.naih.hu

Main areas of responsibility. Among others the Authority:

- Conducts investigations on request.
- Can conduct data protection or 'secret supervisory' administrative procedures on its own initiative.
- Can take a case to the court in the event of violation of law concerning data of public interest and public data on grounds of public interest.
- Keeps the data protection record.
- Issues recommendations on a general basis or on request from a data controller.
- Can carry out data protection audits on request from a data controller.
- Can make recommendations regarding the adoption, modification of laws concerning the processing of personal data and access to data of public interest or public data on grounds of public interest.
- Discloses a yearly report on its own activity until 31 March each year and files it with the parliament.
- Represents Hungary in the data protection supervisory organisations of the EU.

- Processing of personal data without a legal basis or contrary to the purpose of the data processing.
- Failure to take measures serving the security of the data.

The penalty for this offence is up to one year's imprisonment.

Any person not fulfilling the obligation to provide the data subject with information and as a result significantly violating the interest of others is similarly punished.

If an individual commits abuse of personal data in relation to sensitive personal data, the penalty is up to two years' imprisonment. If an individual commits abuse of personal data as an official person or by using a public commission, the penalty is up to three years' imprisonment.

Minor offences are punished by a fine, for example:

- Failure to report, register or provide data required by law.
- Providing false data intentionally.
- Hindrance of the supervision of the respective authority.

Civil law consequences

Data subjects, if their rights are violated or if they disagree with the data controller's decision regarding their objection, can file a civil claim against the data controller. In certain cases the data recipient can file a civil claim against the data controller. If the court rules in favour of the data subject or the data recipient, it obliges the data controller to:



- Provide the data subject with the requested information.
- Rectify, block or delete data.
- Withdraw a decision made by automated technical data processing.
- Consider the data subject's right to object.
- Release the data requested by the data recipient.

The court can make its judgment public if the interest of data protection and the rights protected by law of a greater number of data subjects require it. In the court procedure the data controller bears the burden of proof and must prove that data processing complies with the relevant legislation.

The data controller is liable for damages resulting from unlawful data processing or the violation of data security requirements (with the exception of force majeure and cases when the damage was caused intentionally by the claimant or by the claimant's material negligence).

Administrative consequences

See *Question 24*. As the Authority was established on 1 January 2012, there is not yet any practice or case law about the administrative consequences of a violation of law.

See table, *Sanctions for data breaches*.

CONTRIBUTOR DETAILS



JÁNOS TAMÁS VARGA

VJT & Partners Law Firm

T +36 1 501 9900

E vargajt@vjt-partners.com

W www.vjt-partners.com



ZOLTÁN TARJÁN

VJT & Partners Law Firm

T +36 1 501 9900

E tarjanz@vjt-partners.com

W www.vjt-partners.com

Qualified. Budapest Bar Association, Hungary, 1996

Areas of practice. M&A; private equity; outsourcing; data protection; employment; commercial.

Recent transactions

Providing legal advice for a global financial services provider on a broad range of data protection issues, including:

- The transfer of employees' personal data between different entities of the company group.
- The transfer of insurance and fund secrets.
- Data protection and advertising law issues arising in connection with cross-selling co-operation initiatives.
- Data protection issues arising in connection with the outsourcing of application and hosting services.

Providing legal advice for a multinational IT and payment processing services provider on the applicability and authorisation of binding corporate rules.

Qualified. Budapest Bar Association, Hungary, 2008

Areas of practice. Outsourcing; data protection; IP; communications; e-commerce; commercial.

Recent transactions

Providing legal advice for a global financial services provider on broad range of data protection issues, for example:

- The transfer of employees' personal data between different entities of the company group.
- The transfer of insurance and fund secrets.
- Data protection and advertising law issues arising in connection with cross-selling co-operation initiatives.
- Data protection issues arising in connection with the outsourcing of application and hosting services.

Providing legal advice for a multinational IT and payment processing services provider on the applicability and authorisation of binding corporate rules.