DATA PROTECTION
Hungary

János Tamás Varga and Zoltán Tarján

REGULATION

1. What national law(s) regulate the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The primary legislation regulating the collection and use of personal data is Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (DPA), which implements the Data Protection Directive. The DPA aims to guarantee the right of individuals to exercise control over their personal data and to have access to data of public interest. The DPA is regarded as background legislation for specific statutes regulating the collection and use of personal data.

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 personal 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 XC of 2005 on Freedom of Information by Electronic Means.** The Act aims to ensure continuous and free-of charge electronic access to the defined scope of data of public interest, without identification and data request procedures.
- **Act C of 2003 on Electronic Communications.** 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.
- **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.

2. To whom do the rules apply (EU: data controller)?

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

The DPA defines a data controller as any individual or legal person or any organisation without legal personality that:

- Determines the purpose of the processing of data.
- Makes decisions on data processing (including concerning the means of processing).
- Implements these decisions or has them implemented by a technical data processor (*see below*).

A technical data processor is any individual or legal person or organisation without legal personality that performs the technical processing of personal data on commission given by the data controller, including commission given on the basis of legislation.

The main distinguishing feature is that the data controller determines the purpose of data processing and makes decisions on data processing. The technical data processor, however, can only perform technical tasks related to data processing operations, and to 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.

3. What data is regulated (EU: personal data)?

The DPA defines "personal data" as any data relating to a specific (identified or identifiable) individual (data subject), as well as any conclusion in relation to the data subject which can be inferred from this data. During data

processing, data remains personal data, provided its relation to the data subject can be restored. An individual qualifies as identifiable if, among others, he can be identified, directly or indirectly, by reference to any of the following:

- Name.
- Identification code.
- One or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Personal data under the DPA covers only the personal data of living individuals. However, the term "medical data", regulated under the Medical Data Act covers personal data of living and deceased individuals.

In practice, the Office of the Data Protection Commissioner (Commissioner) interprets personal data broadly (*see box, The regulatory authority*). Even an indirect relationship between the data and the individual is sufficient. 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 data.
- Criminal personal data.
- Data of public interest.
- Public data on grounds of public interest.

See Question 11.

4. What acts are regulated (EU: processing)?

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

- Collection.
- Obtaining.
- Recording.
- Organisation.
- Storage.
- Modification.
- Use.
- Transfer.
- Disclosure.
- Alignment. This is similar to combination, that is, to harmonise or reconcile various personal data.
- Combination.
- Blocking.
- Deletion.
- Destruction.
- Prevention of their further use.

Photographing, sound or image recording, as well as the recording of physical characteristics suitable for the identification of an individual (such as fingerprints and palm prints, DNA samples and iris images) are also considered as data processing.

The DPA goes further than the Data Protection Directive by defining 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.

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*).

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 the Republic of Hungary that either:

- Relates to the data of individuals.
- Contains 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 uses (for the purpose of technical data processing) a technical data processor when either:

- The technical data processor's headquarters, premises or residence is in Hungarian territory.
- Equipment is used that is located in Hungarian territory, except when the equipment is solely used for the transit of data through EU territory.

These data controllers must appoint a representative in Hungarian territory.

According to commentary, the DPA also applies to technical data processing contracts, if the data controller based in Hungarian territory entrusts a technical data processor based outside Hungarian territory with technical data processing.

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

The DPA does not apply to data processing performed by individuals exclusively for their own personal purposes.

Certain legislation (such as the Credit Institutions Act and the Insurance Act) can, on public interest grounds, order or allow the disclosure of personal data for certain purposes (for example for national security, crime prevention or detection and tax authority investigation).

7. Is notification or registration required before processing data? If so, please provide brief details.

Before commencing activities, the data controller must notify the Commissioner, where applicable, of the:

- Purpose of data processing.
- Types of data and the legal basis of data processing.
- Scope of data subjects.
- Source of data.
- Type of the transferred data.
- Recipient of the transferred data.
- Legal basis of the transfer.
- Deadline for deletion of certain types of data.
- 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.
- Name and the contact information of the internal data protection officer.

Any change in the information registered must be notified within eight days.

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

- Involving the data of persons having an employment, membership, student or customer relationship with the data controller.
- 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 data of companies or organs under the Press Law that serve solely their own informational activity.
- Serving an individual's own purposes.

Notification can be performed by completing a notification form in hard copy and in Hungarian. The notification form can be downloaded from the Commissioner's website. Notification is free of charge.

On registration, the data controller receives a registration number, which must be used for every transfer, disclosure and supply of the personal data.

The data protection register, containing the list of data controllers and the relating information registered, can be found on the Commissioner's website.

MAIN DATA PROTECTION RULES AND PRINCIPLES

8. What are the main obligations imposed on data controllers to ensure that 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;
  - 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 processing's purpose;
  - data is accurate, complete and where necessary, kept up-to-date;
  - data is stored in a way that allows identification of data subjects for no longer than it is required for the purpose for which this data is stored.
- **Obtaining consent.** The consent of the data subject must be obtained except if data processing is ordered by a statute or a local government decree (*see Question 9*).

- **Providing information.** Data subjects must be provided with unambiguous and detailed information on all facts relating to the processing of their data (*see Question 12*).
- **Taking technical and organisational measures.** The data controller (and the technical data processor) must ensure data security and take all technical and organisational measures and draw up the procedural rules necessary for compliance with relevant rules on data protection and confidentiality (*see Question 14*).
- **Respecting the rights of the data subjects.** 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 Commissioner.** Before commencing his activity, the data controller must notify the Commissioner of certain information to be registered (*see Question 7*).
- **Appointing an internal data protection officer and drawing up data protection internal regulation.** The data controller and the technical data processor must appoint an internal data protection officer, reporting directly to the head of the organisation for the following organisations:
  - data controllers (or technical data processors) processing (or technical processing) of data files of national authorities, or national labour or criminal data files;
  - financial organisations;
  - telecommunications 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 based outside the EEA (*see Question 16*).

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

- What rules are there concerning the form and content of consent? Does online consent suffice?
- Are there any special rules concerning consent by minors?

The data subject's consent must be obtained, unless data processing is ordered by a statute or a local government decree.

Form and content of consent

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

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

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, particularly in relation to the:

- Purposes and legal basis of the data processing.
- Person authorised to carry out the data processing and the technical data processing.
- Duration of the data processing.
- Person authorised to have access to the data.
- Rights and remedies of the data subject in connection with the data processing.

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 regulation can set out stringent conditions concerning the form of the consent. For example, the Credit Institutions Act requires the authorisation for the transfer of personal data qualifying as bank secrets to be contained in a public deed or in a private document of full probative value, or to be provided in writing within the framework of the conclusion of the contract with the financial institution.

Consent by minors

The DPA does not specifically regulate the form or content of consent by minors. However, the relevant rules of the Civil Code must be considered.

The Civil Code distinguishes between minors under the age of 14 and minors between the age of 14 and 18. 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. Minors aged between 14 and 18

can give their consent to the processing of their personal data. However, the statutory representative's approval must be obtained.

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 if data processing is ordered by a statute or a local government decree. According to the Commissioner's practice, this legal basis can be interpreted more broadly and data processing allowed by statute or a local government decree is deemed lawful.

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

11. Do special rules apply for certain types of personal data, for example sensitive data? If so, please provide brief details.

Any personal data relating to the following qualifies as sensitive personal data (*DPA*):

- Racial, national or ethnic minority origin, political opinion or party affiliation, religious or ideological belief, or membership in any interest group.
- State of health, pathological addictions, sexual life or criminal personal data.

Sensitive personal data can be processed if:

- The data subject has given his written consent.
- This is provided for by a treaty (in case of sensitive personal data specified in the first bullet point above).
- Ordered by a statute.

Information that does not fall under the definition of personal data and is processed by an entity or person performing a state or local government function or other public function, or any information related to these activities, qualifies as data of public interest (*DPA*). Any data that does not fall under this definition, but the disclosure or accessibility of which is ordered by statute on grounds of public interest, qualifies as public data on grounds of public interest (*DPA*). Generally, the DPA provides that entities performing state or local government functions or other public functions must grant individuals access to data of public interest.

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.
- Person authorised to carry out the data processing and the technical data processing.
- Duration of data processing.
- Person authorised to have access to the data.
- Rights and remedies of the data subject in connection with the data processing.

13. What other specific rights (such as a right of access to personal data or the right to object to processing) 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.
- Purpose, legal basis and duration of the data processing.
- Name, address and activity of the technical data processor in connection with data processing.
- Recipients and future recipients of the personal data and the purpose for which they receive the personal data.

The data controller must provide the information in writing and in an easily comprehensible form within 30 days from receipt of the request.

Anyone can inspect the data protection register (*see Question 7*) and take notes or request extracts from it.

The data subject's rights can be restricted by legislation:

- Promoting the interests of the state's external and internal security, such as national defence, national security, crime prevention, criminal investigation.
- Aiming to prevent breaches of labour law or labour safety obligations.

- Aiming to protect the rights of data subjects or of other people.

Right to request rectification or deletion

The data subject can request the rectification or deletion of his personal data (except for data processing ordered by law).

The data controller must rectify any inaccurate personal data.

Personal data must be deleted if:

- The processing of the personal data is unlawful.
- Requested by the data subject (except for data processing required by law).
- It is incomplete or inaccurate and cannot be corrected in a lawful way, provided that 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.
- This has been ordered by the court or the Commissioner.

In particular, legislation to promote the interest of the external and internal security of the state can restrict the rights of data subjects (*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 enforcing the right or legitimate interest of the data controller or data recipient, except if the data processing is required by statute.
- Personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research.
- The right to object is otherwise provided by statute.

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, he can initiate court proceedings.

Right to refer the matter to court or the Commissioner

In case of violation of his rights, the data subject can initiate court proceedings against the data controller (*see Question 21*).

Any individual can refer the matter to the Commissioner if in his opinion, 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 (except when court proceedings have already been initiated (*see Question 20*)).
- There is an imminent danger of violation of his rights.

SECURITY REQUIREMENTS

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

The data controller (and within its scope of activities, the technical data processor) must ensure data security and take all technical and organisational measures. It must draw up the procedural rules necessary for compliance with the DPA and with other rules relating to data protection and confidentiality.

Data must be protected, particularly against:

- Unauthorised:
  - access;
  - alteration;
  - transfer;
  - disclosure;
  - deletion;
  - destruction.
- Accidental destruction or damage.

If personal data is transferred through a network or through other IT equipment, the data controller, technical data processor and operator of the telecommunications or IT equipment must take special protective measures to ensure the technical protection of personal data (*DPA*).

PROCESSING BY THIRD PARTIES

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

Technical data processors (*DPA*):

- 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 data processing operations. The technical data processor is responsible, within the scope of his activities and the framework determined by the data controller, for the following activities in relation to personal data:

- Technical processing.
- Alteration.
- Deletion.
- Transfer.
- Disclosure.
- In performing his tasks, the technical data processor cannot involve other technical data processors.

In addition, companies interested in business activities using the personal data to be technically processed cannot be entrusted with technical data processing. The interpretation of this provision of the DPA is not entirely clear. According to legal commentary, any company which directly uses the personal data in question for its own profit-making purposes cannot be entrusted with the technical processing of personal data.

Contracts on technical data processing must be in writing.

INTERNATIONAL TRANSFER OF DATA

16. 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 EEA. Similarly, no specific restrictions are imposed on the transfer of personal data to Switzerland on the basis of a treaty on the legal status of the citizens of Switzerland.

Personal data (including sensitive data) must not be transferred to data controllers or technical data processors based outside the EEA (and Switzerland) unless (*DPA*):

- The data subject has given his explicit consent.
- This is allowed by a statute 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*):

- The European Commission establishes that the third country ensures an adequate level of protection. Approved destinations are:
  - Argentina;
  - Canada;
  - Faroe Islands;
  - Guernsey;
  - Isle of Man;
  - Jersey;
  - Switzerland;
  - US-based organisations signed up to the Safe Harbor privacy principles.

  Further, adequate level of protection is also ensured for:

  - 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.
- 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 control of data processing and technical data processing.
- The data controller or the technical data processor based in the third country proves (by presenting data processing and technical data processing rules), that he adequately ensures the protection of personal data and the rights of data subjects. This can be deemed to be proved, in particular, when he performs the data processing or technical data processing according to the European Commission's legislation. The use of the standard contractual clauses adopted by the European Commission and the use of binding corporate rules (BCRs) are deemed to ensure an adequate level of protection. In addition, ad hoc contracts on the transfer of personal data to any third country (that do not expressly rely on the standard contractual clauses adopted by the European Commission) can also be deemed to provide an adequate level of protection of personal data.

As an exception, the DPA provides that personal data can be transferred outside the EEA and Switzerland to implement an international legal assistance agreement for the purpose and with the content set out in the agreement.

17. 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 and BCRs are deemed to ensure an adequate level of protection (*see Question 16*).

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

18. 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 or BCRs ensuring an adequate level of protection do not serve as a proper legal basis for transfer of personal data to any third country without satisfying additional requirements since, as a further condition, a statute must allow the data transfer (*DPA*).

If the data subject has provided his explicit consent to the data transfer, there is no requirement for an adequate level of protection (*see Question 9*).

19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

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

ENFORCEMENT AND SANCTIONS

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

The Commissioner supervises compliance with the DPA and other laws on data processing on notification or of its own volition. The Commissioner also investigates complaints filed with him.

On gaining knowledge of unlawful processing of data, the Commissioner must require the data controller to discontinue the data processing.

If the data controller or technical data processor fails to discontinue the unlawful processing (or technical processing) of personal data, the Commissioner can:

THE REGULATORY AUTHORITY

Office of the Data Protection Commissioner
W http://abiweb.obh.hu/abi/

Main areas of responsibility. The Commissioner's responsibilities include:

- Supervising compliance with the DPA and other legislation on data processing on notification or of his own volition.
- Investigating complaints filed with him.
- Ensuring maintenance of the data protection register.
- Promoting the uniform application of statutory provisions on the processing of personal data and on public access to data of public interest.
- Exercising the powers and performing the tasks as set out in the DPA (for example, the Commissioner may issue recommendations).

- Order the blocking, deletion or destruction of data.
- Prohibit the unlawful processing (technical processing) of data.
- Suspend the transfer of data to foreign countries.

The Commissioner can inform the public of the:

- Launch of his investigation.
- Fact of the unlawful processing (or technical processing) of data.
- Identity of the data controller (or technical data processor).
- Scope of data processed as well as the measures initiated and decisions made.

The Commissioner may:

- Request the data controller to supply information.
- Inspect all relevant documents and request copies.
- Have access to all data processing operations.

The Commissioner may enter any premises where data is processed.

21. What are the sanctions and remedies for non-compliance with data protection laws? To what extent are the laws actively enforced?

Criminal consequences

"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 (*Criminal Code*):

- Processing of personal data without 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.

The party not fulfilling the obligation of providing the data subject with information and as a result significantly violating the interest of others is similarly punished. If an individual commits the abuse of personal data in relation to sensitive personal data, the penalty is up to two years' imprisonment.

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

In addition, 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, whose rights are violated, can file a civil claim against the data controller. If the court rules in favour of the data subject, it obliges the data controller to:

- Provide information.
- Rectify or delete data.
- Consider the data subject's right to object.

Under certain circumstances, the court may order the publication of its judgment, including identification of the data controller. The data controller is liable for damages resulting from the unlawful data processing or the violation of the technical requirements of data protection (with the exception of *force majeure* and cases when the damage was caused intentionally or by the claimant's material negligence).

In addition, the data subject may object to the processing of his personal data in cases set out in the DPA (*see Question 13*).

Administrative consequences

See also Question 20.

In 2008, 958 complaints were filed with the Commissioner, who established unlawful data processing in about 60% of cases.