PANORAMIC

DATA PROTECTION & PRIVACY

Hungary

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: August 2, 2024

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Hungary

VJT & Partners

Endre Várady	varadye@vjt-partners.com
János Tamás Varga	vargajt@vjt-partners.com
Andrea Belényi	belenyia@vjt-partners.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The general Hungarian regulatory instruments for the protection of personal information (PI) are the EU General Data Protection Regulation (GDPR) and Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act).

The Data Protection Act was amended in July 2018 to implement the GDPR in Hungary. The Data Protection Act contains provisions spanning three categories:

- provisions applying to data processing that are under the scope of the GDPR. These are additional procedural and substantial rules, where the GDPR permits derogation or the application of national laws;
- provisions applying to data processing operations that fall outside the scope of the GDPR; and
- provisions applying to data processing for law enforcement, national security and national defence purposes to implement Directive (EU) 2016/680 (the Law Enforcement Directive).

Law stated - 13 June 2024

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The authority responsible for overseeing the data protection law is the National Authority for Data Protection and Freedom of Information (the Authority). The Authority has the following investigative powers:

- it may ask for information and request the client to make statements;
- it may take testimony from witnesses (including conducting interviews);
- it may access all PI and information that is necessary for the performance of its tasks;
- it may also ask for copies of PI and other information;
- it may make on-site visits and request access to equipment used in the course of the data processing; and
- it may ask for expert opinions.

Law stated - 13 June 2024

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Authority is a member of the European Data Protection Board (EDPB), which publishes guidelines to ensure consistency across member states in GDPR interpretation. Regarding issues that are covered by guidelines of the EDPB or article 29 of the Data Protection Working Party (the predecessor of the EDPB), the Authority follows those guidelines.

In the case of cross-border data processing, the Authority suspends the proceedings until the lead supervisory authority makes its statements on taking over the case based on the GDPR's one-stop-shop mechanism. In such cases, the lead supervisory authority and the Authority must cooperate to find a mutually acceptable solution. If they cannot, the consistency mechanism applies, in which the EDPB may have the final word.

Law stated - 13 June 2024

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breaches may lead to sanctions, which depend on the type of breach. The most feared sanction is the administrative fine for breaching the GDPR, which may reach €20 million or 4 per cent of the organisation's annual turnover (whichever is higher).

The Authority may also impose corrective measures set out under the GDPR, such as:

- issuing reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR;
- ordering the controller or the processor to comply with the data subject's request to exercise his or her rights;
- ordering the controller or processor to make their processing operations comply with the provisions of the GDPR;
- ordering the controller to communicate a personal data breach to the data subject;
- imposing a temporary or definitive limitation (a ban on processing);
- ordering the rectification or erasure of PI or restriction of processing;
- ordering the suspension of data flows to a recipient in a third country or an international organisation; and
- withdrawing a certification or ordering the certification body to withdraw a certification.

A breach of data protection laws may also lead to criminal penalties if such a breach is committed for financial gain or if it causes significant detriment to individuals. Criminal penalties may include financial penalties, confinement or imprisonment for up to one, two (if

the crime is committed in relation to sensitive or criminal record data) or even three years (if the crime is committed by state officials abusing their powers).

The Authority has two kinds of procedures to handle breaches:

- Investigation: the Authority may start an investigation based on a complaint (which may be made by anyone) or ex officio. At the end of the investigation, the Authority may call on the data controller to remedy the situation. The controller shall remedy the situation within 30 days of receiving the call. In the investigation procedure, the Authority imposes neither a fine nor other corrective measures.
- Administrative procedure: the administrative procedure may be launched based on a complaint (only the concerned data subject may make a complaint) or ex officio. The Authority must launch the administrative procedure ex officio only if in the investigation phase the Authority had imposed an order, but the controller did not remedy the situation within the deadline, or in the investigation phase, the Authority concluded that unlawful processing occurred and based on GDPR rules a fine may be imposed.

Law stated - 13 June 2024

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Yes, PI owners can appeal to the Budapest-Capital Regional Court against the decisions of the Authority.

Law stated - 13 June 2024

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Hungarian data protection laws cover all types of organisations. An exemption applies in the case of individuals processing personal information (PI) for household purposes, but otherwise, any organisation that processes PI will be under the scope of Hungarian data protection laws.

Even when the EU General Data Protection Regulation (GDPR) does not apply (eg, the processing of PI by national security entities or courts), the provisions of Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act) still apply. In such a case, the National Authority for Data Protection and Freedom of Information (the Authority) will remain the supervisory authority with a limited corrective power to impose a fine of up to 20 million forints. In the case of PI processing by the courts, the processing will be supervised by the courts (not the Authority).

As these exemptions are rare, this chapter focuses only on the processes that fall under the scope of the GDPR.

Law stated - 13 June 2024

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Specific Hungarian national legislation covers these areas, such as:

- communications interception: Act XC of 2017 on Criminal Procedure and Act C of 2003 on Electronic Communications;
- electronic marketing: Act XLVIII of 2008 on Commercial Advertisement and Act CVIII of 2001 on Electronic Commerce; and
- the monitoring and surveillance of individuals: Act XC of 2017 on Criminal Procedure and Act CXXXIII of 2005 on Private Security and the Activities of Private Investigators, and numerous other acts depending on which locale the surveillance of individuals takes place (eg, in streets, stadia or vehicles).

Law stated - 13 June 2024

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

Apart from the general data protection framework, there is separate legislation for sector-based data protection rules, including in areas such as marketing, the financial sector, e-commerce, employment, healthcare and research. In April 2019, the Hungarian parliament adopted a GDPR implementation package amending 86 sector-based laws.

Law stated - 13 June 2024

PI formats

What categories and types of PI are covered by the law?

Under the scope of the GDPR, practically all data that provides information about, or in relation to, an identified or identifiable natural person constitutes PI. In addition to the processing of personal data by automated means, Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act) extends the GDPR's application protection also to manual processing, even where personal data is not stored or intended to be stored in a filing system.

Law stated - 13 June 2024

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The reach of law is not limited to PI owners and processors physically established in Hungary. It may also have extraterritorial effect. The Hungarian data protection law applies either:

- when the controller's main establishment is located in Hungary, or the controller's only place of business is in Hungary; or
- when the controller's main establishment is not located in Hungary or the controller's only place of business is not in Hungary, but the controller's or its processor's data processing operation relate to:
    - the offering of goods or services to data subjects located in Hungary, irrespective of whether a payment of the data subject is required; or
    - the monitoring of data subjects' behaviour that occurs in Hungary.

Law stated - 13 June 2024

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All processing (except processing by individuals for household purposes) and all operations on the PI (eg, collection, storage and disclosure) are covered by Hungarian data protection laws.

A distinction is made between the controller who determines the purpose and the means of the data processing and the processor who merely executes the decisions of the controller and processes the PI on behalf of the controller. The processor is not entitled to make any decision on the merits of the data processing.

The controller is primarily responsible for the lawfulness of data processing. However, some obligations directly apply to processors (eg, taking appropriate data security measures) and they may be directly liable if they breach such obligations.

Law stated - 13 June 2024

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

There must be a specific ground on which the controller may hold personal information (PI). Six legal grounds exist:

- the data subject's consent;
- the necessity for the performance of a contract (to which the data subject is party or to take steps at the request of the data subject before entering into a contract);
- the necessity for compliance with a legal obligation to which the controller is subject;
- the necessity to protect the vital interests of the data subject or another natural person;
- the necessity for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; and
- the necessity for the legitimate interests of the controller or by a third party.

In the case of holding special categories of PI, apart from having one of the six legal grounds above, the controller must also check whether one of the conditions of article 9 of the EU Data Protection Regulation applies (eg, the data subject needs to give explicit consent or the processing needs to be necessary to exercise or defend legal claims).

Law stated - 13 June 2024

Legitimate processing – types of PI
Does the law impose more stringent rules for processing specific categories and types of PI?

Apart from the general rules for holding sensitive PI, Hungarian law restricts the processing of certain sensitive PI. The most relevant restrictions include:

- health data may be processed only based on the consent of the data subject or if the controller is authorised to process the data based on the authorisation of Act XLVII of 1997 on the processing of health data and for the purposes defined in the Act;
- employees' biometric data may be processed for identification purposes under limited conditions (eg, unauthorised access would lead to a threat to life or health); and
- employees' or job applicants' criminal data may be processed for vetting purposes only if the applicable Hungarian legislation authorises it, or if it is necessary to protect the employer's significant financial interests, to protect secret information (set by law), or to protect some other specific legitimate interests of the employer (eg, firearms' storage or chemical materials).

Law stated - 13 June 2024

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The EU General Data Protection Regulation (GDPR) applies directly. Controllers must notify data subjects whose personal information (PI) they hold. The notice must contain the elements of article 13 of the GDPR (if PI is obtained from data subjects) or article 14 of the GDPR (if PI is not obtained from data subjects).

The National Authority for Data Protection and Freedom of Information (the Authority) takes a granular approach as it requires detailed notice about the elements of article 13 or 14 of the GDPR on the purpose level. This means that the controller must first define the purpose and then all the relevant information for each data processing purpose must be provided.

The Authority states that the purpose needs to be as specific as possible (eg, 'marketing' is incorrect, as it allows different interpretations, 'sending newsletters' is correct as it allows only one interpretation). If the data was collected for one purpose, in principle, it should not be used for another purpose.

As a general rule, the notice must be provided at the time the PI is collected from the data subject or (if the PI is not directly collected from the data subject) within a maximum of one month after obtaining the PI.

Law stated - 13 June 2024

Exemptions from transparency obligations

When is notice not required?

It is not necessary to notify the data subject about the processing of PI if:

- the data subject already has the information (however, in this case, according to the Authority, the controller must be able to prove that the provision of information has already happened, that all necessary aspects of the data processing have been shared with the data subject and that there has not been any change in the processing);
- the provision of such information proves impossible or would involve a disproportionate effort (in case PI is gathered from sources other than the data subject);
- obtaining or disclosure is expressly laid down by EU or EU member state law to which the controller is subject and that provides appropriate measures to protect the data subject's legitimate interests (in case PI is gathered from sources other than the data subject); and
- when the PI must remain confidential subject to an obligation of professional secrecy regulated by EU or EU member state law, including a statutory obligation of secrecy (in case PI is gathered from sources other than the data subject).

Law stated - 13 June 2024

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

PI must be accurate and kept up to date where necessary. Inaccurate PI must be erased or rectified without undue delay. Healthcare is an exemption where erroneous medical data in the medical record must be erased or rectified in a way that the data originally recorded can be identified.

Law stated - 13 June 2024

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The controller may not collect PI that is unnecessary or irrelevant for the purpose (data minimisation).

If the scope of PI is set by specific national law, then only that PI may be processed. Otherwise, the controller can decide on its own about the amount of PI, but it must be in line with the data minimisation principle.

Law stated - 13 June 2024

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The controller may hold PI only until it is necessary for the purpose (storage limitation).

If specific national law sets the retention periods, those retention periods shall apply. If the law determines the circumstances of processing (such as the scope of PI and authorised persons) but not the duration of processing, the necessity of processing should be reviewed every three years. In other cases, the controller must decide on its own about the duration of processing, but it must be in line with the storage limitation principle.

Law stated - 13 June 2024

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI may only be processed for a specified, explicit and legitimate purpose. The Authority adds that the purpose needs to be as specific as possible (eg, 'marketing' is incorrect, as it allows different interpretations, 'sending newsletters' is correct as it allows only one interpretation).

If the PI was collected for one purpose, in principle it should not be used for another purpose (finality principle).

Exceptions apply from the finality principle in the following cases:

- if the new processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- if the data subject gave consent to the processing for a different purpose; and
- if the processing for a new purpose is based on such EU or EU member state law that aims to achieve certain purposes (eg, home security or public safety) and the processing is necessary and proportionate to the purpose.

If none of the above applies, the controller may carry out a compatibility check according to the GDPR rules to check whether the old purpose is compatible with the new one.

Law stated - 13 June 2024

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Hungarian law does not have a specific, local restriction on the use of PI for making automated decisions (without human intervention). The general GDPR rule (article 22) applies according to which the data subject has the right not to be subject to a decision based solely on automated decision-making, including profiling.

Law stated - 13 June 2024

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The EU General Data Protection Regulation (GDPR) rules apply directly. Both the controller and the processor must implement measures that can prevent personal information (PI) from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. When deciding about the appropriate measures, the controller must consider:

- the state of the art (as technology evolves constantly);
- the costs of implementation of the measures;
- the context of the data processing (eg, its nature, scope and purposes of processing); and
- the associated risks (arising from the data processing) for the rights and freedoms of data subjects.

The burden of deciding what measures are necessary to mitigate the risks is entirely on the controller. But the GDPR itself describes some measures that are advised to be implemented as appropriate:

- the pseudonymisation and encryption of PI;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to PI promptly in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.

The controller is responsible for choosing processors that provide sufficient guarantees to implement adequate technical and organisational measures. To achieve this, the controller must conclude a data processing agreement.

For organisations falling under the scope of Act L of 2013 on the electronic information security of state and local administrative bodies (the Information Security Act), a stricter set of rules applies. Such organisations are placed into one of five categories, depending on the severity of the possible security breach. The categories will require different levels of data security.

Last, the Hungarian implementation of Directive (EU) 2022/2555 on network and information security (the NIS2 Directive) also imposes rules on cyber security risk-management measures and reporting obligations for medium-sized and large businesses in Hungary in various industries including energy, transport, healthcare, pharmaceuticals, manufacturing, chemicals or research. The Hungarian implementation of NIS2 also applies to micro or small businesses in certain specific sectors (eg, communications, trust services, domain name registration).

Law stated - 13 June 2024

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

If a data breach presents a risk to the rights and freedoms of natural persons, the controller must report it to the National Authority for Data Protection and Freedom of Information within 72 hours of gaining knowledge of the data breach. The processor should be obliged in the data-processing agreement to notify the controller about the breach promptly so that the controller can meet the 72-hour deadline.

The controller must also notify the affected natural persons if the processing will likely result in a high risk for the rights and freedoms of those people (eg, physical, material or non-material damages).

Irrespective of whether the notification threshold is reached, the controller must document all relevant information about data breaches. It is also advisable to retain any documentation as proof that the data breach has been handled adequately.

Apart from this general regime, there are some Hungarian sector-specific notification rules:

- providers of electronic communication services must also notify the Hungarian Telecommunication Authority within 24 hours of learning of the breach, and provide a second notification within 72 hours;
- organisations falling under the scope of the Information Security Act must report security incidents (including data breaches) promptly to the central incident management centre (defined in the Information Security Act); and
- organisations falling under the scope of the NIS2 Directive must report security breaches (including data breaches) that have a significant impact on the provision of their services.

Law stated - 13 June 2024

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

A lack of implementation of internal control does not automatically lead directly to EU General Data Protection Regulation (GDPR) sanctions. However, in the lack of such controls, it would be very difficult to ensure and demonstrate compliance with the GDPR requirements and fulfil the accountability principle of the GDPR.

Law stated - 13 June 2024

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

It is not mandatory to appoint a data protection officer (DPO) unless:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale special categories of personal information (PI) and PI relating to criminal convictions and offences.

The DPO's role is mainly supportive and controlling. The officer's primary responsibilities are:

- to inform and advise the controller or the processor and the employees who carry out processing about their obligations under data protection laws;
- to monitor compliance with data protection laws (eg, collecting information about processing, checking the compliance of processing and issuing recommendations on compliance);
- to provide advice on the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing; and
- to assist in maintaining the records of processing activities (although not an explicit legal obligation, it is recommended as best practice).

The DPOs must have the specialised knowledge and the abilities to be able to fulfil their tasks listed above.

The National Authority for Data Protection and Freedom of Information (the Authority) must be notified of the DPO's engagement, and it publishes the contact information of the DPO (name, address, respective controller and/or processor).

Law stated - 13 June 2024

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Both controllers and processors are required to maintain the internal records of processing (ROP) under article 30 of the GDPR. An exemption from this obligation applies in the case of an organisation employing fewer than 250 persons, but only if:

- the processing is occasional (which is rare);
- the processing does not result in a risk to the rights and freedoms of data subjects; and
- sensitive PI or PI relating to criminal data are not processed.

As ROP gives an overall picture of the data processing of an organisation in terms of compliance, the Authority may start an investigation by asking for it.

As, under the accountability principle, the controller must be able to demonstrate compliance with data protection legislation, it is also advisable to implement internal data protection policies as well as other documentation (eg, privacy policies, legitimate interest tests and consent forms).

Law stated - 13 June 2024

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Controllers must undertake a privacy impact assessment (PIA) in relation to certain uses of PI to mitigate the risks arising from high-risk data processing. The Authority has published a list of typical cases in which a PIA is mandatory (eg, large-scale profiling or systematic monitoring). Controllers may decide on the PIA methodology on their own, but the Authority recommends the Hungarian version of the French data protection authority's PIA software.

Law stated - 13 June 2024

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

The GDPR processing rules apply in Hungary, which include:

- privacy by design: controllers must consider the key data protection concern issues such as pseudonymisation or data minimisation via appropriate technical and organisational measures in the early stages of the processing (at the time of deciding on processing) and through the whole life cycle of the data processing; and
- privacy by default: controllers must take appropriate measures so that data processing by default is limited only to a strictly necessary extent, particularly regarding the amount of PI collected, the duration of the processing and access rights.

An approved certification mechanism pursuant to article 42 of the GDPR may be used as an element to demonstrate compliance with the requirements of privacy by design and by default.

Law stated - 13 June 2024

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Controllers or processors are not required to register their data processing with the National Authority for Data Protection and Freedom of Information (the Authority). This obligation ceased in Hungary when the EU General Data Protection Regulation (GDPR) entered into force.

Law stated - 13 June 2024

Other transparency duties
Are there any other public transparency duties?

There are other public transparency duties, such as:

- notification to the Authority about the data protection officer's contact details as the Authority manages an official register on DPOs; and
- sector-specific transparency obligations, such as the obligation of the employer to disclose its whistle-blowing operation on its website or the CCTV operators' obligation to place an adequate camera sign.

Law stated - 13 June 2024

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers
How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The rules on the transfer of personal information (PI) depends on the qualification of the service provider:

- if the service provider acts solely based on the transferor's instructions it will be qualified as a processor. In such case, the transferor must conclude with the service provider a data-processing agreement, under EU General Data Protection Regulation (GDPR) rules. The data subject must be notified about the essential details of such processor (eg, its name, location of processing and type of processing activity);
- if the service provider decides on an important outsourced function on its own independently it may be qualified as a controller. In such case, transfer of PI must be based on proper legal grounds and the data subject must be notified about the details of such transfer; and
- if the service provider decides on an important outsourced function jointly with the transferor, a joint controllership agreement must be concluded and the essence of the agreement must be made available to data subjects.

Law stated - 13 June 2024

Restrictions on third-party disclosure
Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under the Hungarian data protection practice, disclosure of PI (ie, providing PI access to several persons) is prohibited, unless the data subject gives his or her consent or the PI relates to public affairs (eg, the PI relates to the exercising of a public function of a person, and not his or her private life).

Controllers must take measures that, by default, PI cannot be accessed by natural persons without the intervention of the individual identified. Unauthorised disclosure of PI may qualify as a data breach.

Law stated - 13 June 2024

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

PI may only be transferred outside the European Economic Area (EEA) to countries that provide an adequate level of protection according to the adequacy decisions of the European Commission (eg, Canada, Switzerland, New Zealand, Argentina and Japan). On 10 July 2023, the European Commission also brought an adequacy decision in relation to the EU-USA Data Privacy Framework. This means transfers of PI are permitted 'per se' to those US companies that are on the Data Privacy Framework List.

In the case of other non-EEA countries (or US companies not listed on the Data Privacy Framework List), the transfer of PI is permitted only if it is based on appropriate data protection safeguards or if a derogation applies.

Safeguards may include the following legal instruments:

- standard contractual clauses (SCCs) approved by the European Commission;
- binding corporate rules (BCRs) for transfers within international company groups;
- a code of conduct that is officially approved according to GDPR rules;
- a certification mechanism that is officially approved according to GDPR rules; and
- an individual transfer agreement approved by the National Authority for Data Protection and Freedom of Information (the Authority).

The ***Schrems II*** decision (Case C-311/18) of the Court of Justice of the European Union (CJEU) is still a milestone decision as it has key takeaways for using data protection safeguards in relation to transfers of PI outside the EEA.

The CJEU made it clear that it is not sufficient just to rely on the paperwork in the context of safeguards (eg, just signing the SCC). The controller must factually assess and document to establish if the level of protection required by EU law is respected in the third country before determining whether the guarantees provided by the safeguards (eg, by the SCCs or BCRs) can be complied with in practice (eg, whether the access to PI by public authorities is not a disproportionate measure). If not, the controller must assess whether by providing supplementary measures the adequate level of protection can be met (eg, by the encryption of PI, which would make access to the PI by public authorities meaningless).

If an adequate level of protection could not be met, the controller may still transfer the PI if any derogations apply. Derogations may be:

- the data subject gives his or her explicit, specific and informed consent to the transfer;
- the transfer is objectively necessary for the performance of the contract with the data subject;

- the transfer is necessary to protect the vital interests of an individual;
- the transfer is necessary for the public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- the transfer is necessary for the compelling and overriding legitimate interests of the controller (under limited conditions such as the transfer is not repetitive and applies only to a limited number of data subjects).

The scope of these derogations is specified in European Data Protection Board Guideline No. 2/2018.

Law stated - 13 June 2024

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The cross-border transfer rules apply equally to every form of transfer, irrespective of whether it is a controller-controller, a controller-processor or an onward transfer. Additionally, the same regime applies to data transfers to international organisations as well.

Law stated - 13 June 2024

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No, in general the law does not require PI or a copy of PI to be retained in Hungary. However, certain organisations falling under the scope of the Information Security Act (such as certain public bodies and data processors of certain public records) must retain data in Hungary and may not transfer it to other countries. Similarly, data localisation requirements apply to online betting service providers according to the Gambling Act as they have to establish their servers in Hungary.

Law stated - 13 June 2024

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals may ask the controller to obtain a copy of their personal information or to obtain supplementary information about the processing of their personal information.

Individuals do not have to justify why they want to exercise their right to access. However, certain limitations still apply to this right:

- the controller may request the individual to identify him or herself if, for example, the request is submitted orally or by email, but the controller has reasonable doubts about the identity. If the individual does not identify him or herself, the controller may refuse the request;
- the controller may request the individual to specify his or her request;
- the controller may refuse the request if it is manifestly unfounded or excessive (but, according to the National Authority for Data Protection and Freedom of Information (the Authority), in both cases the controller may not refuse the request if the administrative cost of fulfilling the request is trivial) or charge a reasonable fee taking into account the administrative cost; and
- the right to access may not adversely affect the rights and freedoms of others (eg, personal information (PI) of other data subjects or trade secrets).

When refusing an access request or deciding to charge a reasonable fee, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Law stated - 13 June 2024

Other rights

Do individuals have other substantive rights?

Individuals have other substantive rights under the EU General Data Protection Regulation (GDPR) framework. Individuals may:

- request the erasure of the PI in some circumstances (if, for example, the PI is no longer necessary for the purpose);
- request the rectification of the PI, if the PI is inaccurate or incomplete;
- the restriction of the PI, meaning that the controller may only store the PI (if, for example, the PI is no longer necessary for the purpose, but the data subject needs it for legal claims);
- object to the data processing, if the processing is based on legitimate interest and the data subject's interest overrides the interest of the controller;
- the exporting of their PI (ie, receiving the PI in a portable format or directing the controller to transmit the PI to another controller); and
- not be subject to decisions based solely on automated decision-making.

Individuals have the right to compensation should a controller breach their rights under the GDPR.

Law stated - 13 June 2024

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals may claim both material damages covering the actual damage and non-material damages covering injury to feelings and violation of personality rights. Controllers and processors must be able to prove that the breach of data protection laws has not occurred.

In its decision C-300/21, the Court of Justice of the European Union held that while an infringement of the GDPR and resulting material or non-material damage are required for the right to compensation, a certain 'seriousness' threshold cannot be imposed as a prerequisite for such compensation. The judgment directs to member states' national laws to specify the rules on the criteria for determining the extent of any compensation payable.

Law stated - 13 June 2024

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals may claim damages only before the court, but other rights may be enforceable before both the Authority and the court. In addition, parties can turn to court to challenge the decisions of the Authority.

Law stated - 13 June 2024

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Data Protection Act) establishes the possibility of exercising some data subject rights (ie, the rights of access, rectification, erasure, restriction of the processing and to object) on behalf of deceased persons. Five years after the death of the data subject, the close relative or the authorised person of the data subject may exercise certain data subject rights under the conditions set out in the Data Protection Act.

Law stated - 13 June 2024

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The National Authority for Data Protection and Freedom of Information (the Authority) issued some guidance about using cookies. The most important rules are the following:

- the user must be informed about the cookies. Practically, a pop-up message should appear during the first visit to the website, which should contain the link in which the full information about the cookie is accessible;
- non-functional cookies, which are not essential for the website operation, such as marketing or analytical cookies, shall be placed on the user's device only based on the user's prior informed and explicit consent;
- functional cookies, which are essential for the website's operation (eg, without them the communication through the website would not work) may be placed on the user's device without his or her consent. But a legitimate interest test must be conducted to prove that the website operator's interest in placing the cookies is stronger than the user's privacy interest; and
- the website operator is liable for the third-party cookies on its website; thus it should use only those third-party cookies that it has full knowledge of.

The European Data Protection Board (EDPB), in its updated guidance on consent (Guidelines 05/2020 on consent), adds that the use of access to services and functionalities must not be made conditional on the consent for the use of cookies (which means that cookie walls are not acceptable). In January 2021, the Authority also stated how the website operators shall use embedded social media modules on their website. As website operators process the personal data of users by embedding tracking pixels (as this process enables the transfer of users' personal data to the social media provider), the Authority requires website operators to comply with the prior privacy notice and free consent requirements. The Authority relies on EDPB Guidelines 08/2020 on the targeting of social media users.

In January 2023, the EDPB published a report of the work undertaken by its Cookie Banner Taskforce, in which it provided guidelines concerning the subsequent processing activities undertaken by the data controller (ie, the data processing that takes place after storing or gaining access to information stored in the terminal equipment of a user, for example, the placement or reading of cookies).

Law stated - 13 June 2024

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Under the Hungarian law on advertising, sending unsolicited electronic marketing (via email, fax or text) is permissible only if the prior, explicit and unambiguous consent of the recipient has been obtained. However, the Authority, in its guideline, recognised that based on the EU General Data Protection Regulation (GDPR) it is permissible to send direct marketing communication if:

- it is directed at existing clients;
- it relates to similar products and services;
- the client has the possibility to opt out from future communication; and
- the sender performs and documents the legitimate interest test in which it explains why its business interest overrides the client's interest.

In the case of voice-to-voice calls, an individual may be called only if he or she has not objected to such communication (eg, in the relevant publicly available phone directory there is no indicator showing that the person does not wish to receive marketing calls). In the case of automated calls, the holder of the phone number must give his or her prior explicit consent to receive the call (eg, in the phone subscription contract).

Law stated - 13 June 2024

Targeted advertising

Are there any rules on targeted online advertising?

The GDPR is directly applicable; there is no specific local requirement.

Law stated - 13 June 2024

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

The Authority argues that, in the case of holding special categories of personal information, apart from having one of the six legal grounds, the controller must also check whether one of the conditions of article 9 of the GDPR applies (eg, the data subject needs to give explicit consent or the processing needs to be necessary to exercise or defend legal claims).

Law stated - 13 June 2024

Profiling

Are there any rules regarding individual profiling?

The GDPR is directly applicable, there is no specific local requirement.

Law stated - 13 June 2024

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

There is no specific Hungarian legislation explicitly regulating cloud computing, and the Authority has no guidance about it either. Controllers, however, are advised to adhere to European best practices (eg, article 29 Data Protection Working Party Opinion on Cloud Computing).

Further, the Central Bank of Hungary (CBH) issued guidance (effective from 1 May 2019) on how financial institutions should use social and public clouds. The guidance, among others, contains rules on the minimum elements of cloud service agreements, risk analysis, implementation of cloud systems, control mechanisms, exit strategy and notification to the CBH.

Law stated - 13 June 2024

UPDATE AND TRENDS

Key developments of the past year
Are there any emerging trends or hot topics in international data protection in your jurisdiction?

As of January 2024, the Hungarian implementation of the NIS2 regulation entered into force. Many middle-sized and large companies are affected in various industries. This imposes a various new task for businesses in the data security area, among other things:

- working out information security systems, cyber security management processes and a business continuity plan;
- carrying out proper risk analysis;
- designating the information security chief;
- putting in place by the relevant business units to prevent, detect, manage, report, and mitigate the effects of security incidents;
- ensuring that the cybersecurity requirements are reflected in the service contracts throughout the whole supply chain; and
- raising cybersecurity awareness through education.

Businesses will have to be wary of meeting the key deadlines:

- registration by the cybersecurity regulator: 30 June 2024;
- working out the appropriate security measures: 18 October 2024;
- signing the contract by the cybersecurity auditor: 31 December 2024; and
- conducting the first cybersecurity audit: 31 December 2025.

Law stated - 13 June 2024