Global Data and Cyber Handbook - Hungary

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

In 2024, the most significant legal development regarding data privacy and cybersecurity on a national level was the implementation of the NIS 2 Directive into Hungarian law: Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision, “Cyber Certification Act” entered into full force on 18 October 2024. At the end of 2024, the Hungarian Parliament enacted a new cybersecurity law in Hungary. Act LXIX of 2024 on Hungary’s Cybersecurity repeals the Cyber Certification Act and Act L of 2013 on the Electronic Information Security of the State and Local Municipality Organizations. Together with Government Decree No. 418/2024 (XII. 23.) on the Implementation of the Cybersecurity Act, the Cybersecurity Act provide a new framework for Hungarian cybersecurity regulation. While we have noticed a continuing focus on data protection requirements regarding the use of cameras, CCTV-surveillance, and the provision of adequate information about data processing based on the Hungarian Data Protection Authority's decisions, other authorities have shifted focus towards cybersecurity.

This chapter has been reviewed and updated on 30 December 2024.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: December 2024*

 omnibus — all personal data

sector-specific — e.g., financial institutions, governmental bodies

constitutional

## What are the key data privacy laws and regulations?

*Last review date: December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide cybersecurity and other data-related legislation.*

[EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679)

[Fundamental Law of Hungary](https://net.jogtar.hu/jogszabaly?docid=a1100425.atv) (25 April 2011)

[Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information](https://net.jogtar.hu/jogszabaly?docid=A1100112.TV) (Information Act)

[Act XLVII of 1997 on Processing and Protection of Medical and Other Related Personal Data](https://net.jogtar.hu/jogszabaly?docid=99700047.TV)

[Act LIII of 2018 on the Protection of Privacy](https://net.jogtar.hu/jogszabaly?docid=A1800053.TV)

[Act C of 2003 on Electronic Communications](https://net.jogtar.hu/jogszabaly?docid=A0300100.TV)

[Act CI of 2023 on the System for the Exploitation of National Data Assets and on Certain Services](https://net.jogtar.hu/jogszabaly?docid=A2300101.TV&amp;celpara=&amp;searchUrl=/jogszabaly-kereso?sorszam%3D101%26para%3D%26tipus%3D%26evszam%3D2023)

[Act XXV of 2023 on Complains and Public Interest Disclosures, and on the Rules of Whistleblowing Notifications](https://net.jogtar.hu/jogszabaly?docid=A2300025.TV&amp;searchUrl=/gyorskereso?keyword%3D2023%252025%2520tv)

## What are the key cybersecurity laws and regulations?

*Last review date: December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide cybersecurity and other data-related legislation.*

[EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679)

[Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&amp;qid=1735549087492)

[Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&amp;qid=1735549131220)

[Commission Implementing Regulation (EU) 2018/151](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0151&amp;qid=1735549177377)

[Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information - Information Act](https://net.jogtar.hu/jogszabaly?docid=A1100112.TV&amp;searchUrl=/gyorskereso?keyword%3Dinfo%2520tv)

[Act CVIII of 2001 on Electronic Commercial Services and Certain Matters regarding Information Society Services](https://net.jogtar.hu/jogszabaly?docid=A0100108.TV&amp;searchUrl=/gyorskereso?keyword%3D2001%2520108%2520tv)

[Act C of 2003 on Electronic Communications](https://net.jogtar.hu/jogszabaly?docid=A0300100.TV&amp;searchUrl=/gyorskereso?keyword%3D2003%2520100%2520tv)

[Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities](https://net.jogtar.hu/jogszabaly?docid=A0700138.TV&amp;searchUrl=/gyorskereso?keyword%3D2007%2520138%2520tv)

[Act CXX of 2001 on the Capital Market](https://net.jogtar.hu/jogszabaly?docid=A0100120.TV&amp;searchUrl=/gyorskereso?keyword%3D2001%2520120%2520tv)

[Government Decree no 42 of 2015 (III. 12.) on the Protection of Information Technology Systems of Financial Institutions, Insurance and Reinsurance Undertakings, Investment Firms and Commodity Dealers](https://net.jogtar.hu/jogszabaly?docid=A1500042.KOR&amp;searchUrl=/gyorskereso?keyword%3D2015%252042%2520korm)

[SZTFH Decree 10/2023 (V. 15.) on the cybersecurity certification of the information and communication technologies](https://net.jogtar.hu/jogszabaly?docid=A2300010.STF&amp;searchUrl=/gyorskereso?keyword%3D2023%252015%2520sztfh)

[SZTFH Decree no. 15 of 2023 (VII. 31.) on the Administrative Service Fees of the Procedures of the Supervisory Authority of Regulated Activities Regarding its Cybersecurity Tasks](https://net.jogtar.hu/jogszabaly?docid=A2300015.STF&amp;searchUrl=/gyorskereso?keyword%3D2023%252015%2520sztfh)

[Regulation (EU) 2022/2554 on digital operational resilience for the financial sector](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&amp;qid=1735549861019)

[MK Decree No. 7/2024 (VI. 24.) on the Requirements for Security Classification and the Specific Security Measures to be applied for Each Security Class](https://net.jogtar.hu/jogszabaly?docid=A2400007.MKF&amp;searchUrl=/gyorskereso?keyword%3D7/2024%2520MK)

[SZTFH Decree No. 7/2024 (VI. 24.) on the Registry of Auditors Authorized to Conduct Cybersecurity Audits and the Requirements for Auditors](https://net.jogtar.hu/jogszabaly?docid=A2400007.STF&amp;searchUrl=/gyorskereso?keyword%3D7/2024%2520sztfh)

[SZTFH Decree no. 10 of 2024. (VIII. 8.) on the National Cybersecurity Certification Scheme for IoT Devices](https://net.jogtar.hu/jogszabaly?docid=A2400010.STF&amp;searchUrl=/gyorskereso?keyword%3D10/2024%2520sztfh)

[Act LXIX of 2024 on Hungary’s Cybersecurity (“Cybersecurity Act”)](https://magyarkozlony.hu/dokumentumok/6b0e9bfc268548e6fc978a3760f0b0b97961c19f/megtekintes)

[Government Decree No. 418/2024 (XII. 23.) on the Implementation of the Cybersecurity Act](https://magyarkozlony.hu/dokumentumok/e7e18faa6e313ad8b8b59e8df094398994cbd967/megtekintes)

## What are the key laws and regulations relating to non-personal data?

*Last review date: December 2024*

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information - Information Act

Act CVIII of 2001 on Electronic Commercial Services and Certain Matters regarding Information Society Services

Government Decision 1507/2023 (XI. 22.) on the measures necessary for the application of Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance and amending Regulation (EU) 2018/1724

Government Decree 250/2024 (VIII. 15.) on the Tasks of the National Agency for Data Assets and on Data Utilisation Support Services

Act L of 2013 on the Electronic Information Security of the State and Local Municipality Organizations (effective until 31 December 2024)

Act CI of 2023 on the System for the Exploitation of National Data Assets and on Certain Services

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: December 2024*

Yes. The Cybersecurity Act will repeal, as of 1 January 2025, the Cyber Certification Act and Act L of 2013 on the Electronic Information Security of State and Local Government Bodies and, together with its implementing government decree, Government Decree No. 418/2024 (XII. 23.) on the Implementation of the Cybersecurity Act, provide a new framework for Hungarian cybersecurity regulation.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: December 2024*

The data protection authority in Hungary is the National Authority for Data Protection and Freedom of Information (in Hungarian: *Nemzeti Adatvédelmi és Információszabadság Hatóság,* "**NAIH**") ([www.naih.hu](http://www.naih.hu/)).

The Hungarian Competition Authority (in Hungarian: *Gazdasági Versenyhivatal*, "**GVH**") might also investigate compliance with data privacy laws and non-personal data laws from the consumer protection perspective.  The GVH launched a market analysis on the impact of artificial intelligence.

With respect to Whistleblowing channels, the Hungarian Employment Supervisory Authority (in Hungarian: *Foglalkoztatás Felügyeleti Hatóság*) may monitor compliance with the relevant rules.

Further, the Hungarian authorities listed below may enforce sector-specific data privacy and data security rules:

in the TMT sector, the National Media and Infocommunications Authority (in Hungarian: *Nemzeti Média- és Hírközlési Hatóság* ("**NMHH**") ([nmhh.hu](http://www.nmhh.hu/)) enforces the special provisions relating to the processing of subscriber data, including security incident reporting obligations, and special data security requirements;

in the financial sector, the Hungarian National Bank (in Hungarian: *Magyar Nemzeti Bank,* "**MNB**") ([mnb.hu](http://www.mnb.hu/)) acts as the financial supervisory authority and is responsible for enforcing the special rules of (i) information security requirements for financial institutions; (ii) outsourcing for credit institutions, as well as for insurance and reinsurance companies; and (iii) security incidents of payment service providers;

with respect to information society services, providers of services subject to notification under Act CVIII of 2001 on Electronic Commerce and on Information Society Services must comply with special information security requirements and report security incidents to the National Security Service (in Hungarian: *Nemzetbiztonsági Szakszolgálat*; "**NBSZ**") ([nbsz.gov.hu](http://www.nbsz.gov.hu/));

regarding entities that fall under the scope 1. § (1) a)-c) of the Cybersecurity Act (formerly these entities fell under the scope of Act L of 2013 on the Electronic Information Security of the State and Local Municipality Organizations), the National Security Service (see above) is responsible for supervising compliance with special information security requirements and the fulfilment of security incident reporting obligations.;

in relation to national data assets, the National Data Agency (in Hungarian: *Nemzeti Adatvagyon Ügynökség*, “**NAVÜ**”) is responsible for facilitating the use of public data, personal data and proprietary data that form part of the national data assets held by public sector bodies under the data asset utilization system; and

regarding entities that fall under the scope of on the Cybersecurity Act, the Regulatory Authority for Regulated Activities (in Hungarian: *Szabályozott Tevékenységek Felügyeleti Hatósága*, “SZTFH”) ([sztfh.hu](https://sztfh.hu/)) is the certification body, responsible for monitoring the development of the European certification scheme and the supervision of the national cybersecurity certification scheme.

## How active is each of the regulator(s)?

*Last review date: December 2024*

Moderately active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: December 2024*

**NAIH**

The NAIH has not yet published its annual report regarding 2024 and its enforcement priorities for the 2025 calendar year. However, based on the NAIH's decisions published in the last 12 months, the NAIH has been especially focused on: (i) the practice of controllers in relation to providing adequate notification to the data subject; and (ii) data protection requirements regarding the use of new technologies, such as artificial intelligence, and the use of cameras and CCTV-surveillance.

In the last 12 months, the most remarkable data protection related cases were the following:

In relation to a IT service provider operating a system used in public educational institutions as a data processor, the NAIH imposed a fine of HUF 110,000,000 (approximately EUR 268,000) for noncompliance with the GDPR. Some issues highlighted by the NAIH, were that the service provider did not adequately take into account the risks arising from the data processing in the data security settings of its IT development environment and failed to notify a personal data breach to the data controllers without undue delay after becoming aware of it. The NAIH also highlighted that the requirement of data security should be enhanced in the case of such a system, as it involves the storage of a large amount of personal data involving a large number of data subjects.

The NAIH imposed a fine of HUF 80,000,000 (approximately EUR 195,000) on a hypermarket operator because the operator , inter alia, (i) did not display an adequate privacy notice containing relevant information about the actual data processing; (ii) during the verification of customers’ ages, it exceeded the scope of its relevant legal obligation as a legal basis for the data processing by recording data in the log files when entering its customers’ personal data into the register system; and (iii) failed to establish adequate measures within each store to protect the personal data of the data subjects, as store employees did not follow the stated procedures when asking customers to state their birth date in circumstances in which that date was clearly audible to others.

The NAIH imposed a fine of HUF 60,000,000 (approximately EUR 146,000) on a bank for unlawful data processing related to the use of cameras in its branches. In the case, the NAIH found that the sticker displayed in the bank's branches contained only a warning about data processing by cameras and did not contain sufficient information about the data processing (e.g., its purpose, legal basis, duration, and the rights of data subjects), thereby breaching the information obligation provisions of the GDPR. The NAIH also found it unlawful that (i) the full privacy notice was not available to customers using ATMs outside opening hours, as it was not available on the website; and that (ii) the bank did not timely comply with a data subject's request for a copy of their personal data and the request to restrict data processing.

The NAIH imposed a fine of HUF 10,000,000 (approximately EUR 24,000) in an administrative proceeding for data protection concerning unlawful data processing and the infringement of data subjects' rights in relation to news articles published on the internet. In that case, the NAIH explained that, in its view, the natural person applicant (**"Applicant"**) could qualify as a public figure because of their public policy statements; however, the fact that the Applicant's spouse is a person entrusted with public functions as mayor and a public figure as a politician it is not sufficient for the purposes of determining that the Applicant has the status of a public figure .

In another case the NAIH fined the Mayor’s Office of Kerepes of HUF 8,000,000 (approximately EUR 19,550) for unlawful data processing in relation to the public surveillance system's camera recordings in the territory of the relevant town. In that case, the NAIH stated that the access to and availability of recordings made by a public camera is subject to strict rules detailing who is entitled to carry out data processing operations.

In various other cases, the NAIH imposed fines on companies ranging between HUF 1,000,000 (approximately EUR 2,500) and HUF 5,000,000 (approximately EUR 12,200) for other infringements of the GDPR, such as the lack of justification of legal bases and inadequate provision of information on data processing.

**NMHH:**

The NMHH has not yet published its annual report regarding 2024 and its enforcement priorities for the 2025 calendar year. However, the NMHH participated in research focusing on awareness of online data processing among internet users with the Data Driven Marketing Association (in Hungarian: "*Adatvezérelt Marketing Szövetség*").

**MNB**:

The MNB published a report on Fintech and digitalization, in which it highlighted that continuous improvement is needed to address growing cybersecurity risks in relation to the digitalization of business operations. The MNB also published an article examining the ethics of artificial intelligence in the context of the digital transformation of the domestic financial sector and another article on banking opportunities and challenges with the emergence of AI. The MNB also participates in the *KiberPajzs* (**"Cybershield"**) program together with *inter alia,* the NMHH, the SZTFH and the NBSZ, which focuses on enhancing digital security.

The MNB also published a Prudential Audit Plan for 2025, in which it identifies the priorities of upcoming audits as being, *inter alia*, (i) exploring the use of machine learning and artificial intelligence; (ii) the use of cloud services; and (iii) examining IT tools for fraud prevention.

**NBSZ**:

Within the organization of the NBSZ, the National Cyber Defense Institute (in Hungarian: *Nemzeti Kibervédelmi Intézet* ("**NKI**")) is an institute established to conduct the operational tasks with regard to the information systems of the state and local government organizations. In 2024, the NBSZ organized an awareness campaign in relation to fraudulent bank calls, fake news, fake links, password safety and multi-factor authentication.

**SZTFH:**

In 2024, the SZTFH identified strengthening cybersecurity and raising cybersecurity awareness as one if it's top priorities. During the year of 2024 the SZTFH organized cybersecurity event series, such as an education campaign on current cybersecurity threats to businesses.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

Common

Class actions/group actions under data or cyber regulation are:

Not available in the jurisdiction

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: December 2024*

There are:

**Administrative remedies / civil penalties applied by regulators and law enforcement**

Administrative fines can amount to up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Private individuals may file complaints with the NAIH.

Data subjects may submit claims for grievance fees to a court.

**Criminal penalties from regulators and law enforcement**

**Misuse of Personal Data:** Under Sections 219 (1)-(4) of Act C of 2012 on the Hungarian Criminal Code, any person who, in violation of the statutory provisions governing the protection and processing of personal data and the provisions set out in binding legislation of the European Union:

is engaged in the unauthorized and inappropriate processing of personal data; or

fails to take measures to ensure the security of data,

with gainful interest or thus causing a significant injury of interest, is guilty of a misdemeanor punishable by imprisonment not exceeding one year.

Said penalty may be imposed on any person who, in violation of data protection laws fails to notify the data subject as required with a view to exercising his rights of access, and thereby imposes significant injury to the interests of another person or persons.

Any misuse of personal data shall be punishable by imprisonment not exceeding two years if committed in connection with special data or personal data from criminal records.

Where a felony occurs because the misuse of personal data is committed by a public official or in the course of discharging a public duty, the penalty is imprisonment not exceeding three years. In addition to that, other criminal offences might be relevant, e.g., illicit access to data and breach of information systems and mail fraud.

**Related crimes under Hungarian law:**

**Information System Fraud** (Section 375 of the Criminal Code)

Any person who, for unlawful financial gain, introduces data into an information system, or alters or deletes data processed therein, or renders data inaccessible, or otherwise interferes with the functioning of the information system, and thereby causes damage, is guilty of a felony punishable by imprisonment not exceeding three years.

**Illicit Access to Data** (Section 422 of the Criminal Code)

Any person who, for the purpose of unlawfully gaining access to personal data, private secrets, trade secrets or business secrets:

covertly opens or obtains the postal consignment or other sealed consignment which belongs to another, and records such by technical means

intercepts communications, by way of electronic surveillance of electronic communications networks or equipment, so as to secretly gain access to communications through information systems, and record its findings using technical devices

secretly gains access to data stored in information systems, and record its findings using technical devices

is guilty of a felony punishable by imprisonment not exceeding three years.

**Private remedies**

Individuals may, for example claim damages for material or non-material (grievance fee) damages

If data subjects have private remedies, what form can these remedies take?

individual personal actions

## If data subjects have private remedies, what form can these remedies take?

*Last review date: December 2024*

N/A

# Key Definitions

## Personal data

*Last review date: December 2024*

Personal data means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: December 2024*

Sensitive data includes:

personal data revealing racial or ethnic origin

personal data revealing political opinions

personal data revealing religious or philosophical belief

personal data revealing trade / professional union or association membership

genetic data

biometric data for the purpose of uniquely identifying a natural person or biometric templates

data concerning health/medical information

data concerning a natural person's sex life or sexual orientation

personal data regarding an individual's criminal convictions or record

Note: financial information does not qualify as special personal data under the GDPR, but — under the practice of the NAIH — the breach of confidentiality of this category of personal data may result in a severe risk to the rights and freedoms of the data subjects. Therefore, should a personal data breach occur relative to this type of data, the NAIH would treat said event similarly to a data breach relative to special categories of personal data.

## Controller vs Processor

*Last review date: December 2024*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Answer:** Yes

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: December 2024*

applies to organizations located in the jurisdiction

applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction

applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: December 2024*

Yes.

The following are potential legal bases for processing personal data:

the data subject has provided consent to the processing for the identified purposes

the personal data is necessary to perform a contract with the data subject

the personal data is necessary to comply with a legal obligation

the personal data is necessary to protect the vital interests of a natural person

the personal data is necessary for a public interest

the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: December 2024*

Yes.

The following are potential legal bases for processing special categories of personal data:

the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

processing relates to personal data which are manifestly made public by the data subject

processing is necessary for the establishment, exercise or defense of legal claims

processing is necessary for reasons of substantial public interest

processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

processing is necessary for reasons of public interest in the area of public health

processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

other

On the basis of Article 9(4) of the GDPR, the Act XLVII of 1997 on Processing and Protection of Medical and Other Related Personal Data contains additional legal bases for the processing of personal data concerning health.

These include data processing:

promoting the preservation, improvement and maintenance of health

promoting the provision of effective medical treatment to the patient, including professional supervision

monitoring the health of the data subject

conducting measures necessary for public health and epidemiological purposes;

enforcing patient rights

for the specific purposes expressly permitted by Hungarian legislation (such as: the training of health care professionals, medical and epidemiological examination, analysis, planning, organization of health care, and planning of costs; statistical analysis; anonymization for impact assessment; scientific research; determination of social security and social benefits; law enforcement; administrative procedure; court proceedings; monitoring, measuring and evaluating the performance of the health system; pharmacovigilance; etc.), or

with the written consent of the data subject

One of the above legal bases must be applied in addition to the legal bases listed in Article 9(2) of the GDPR.

Under the Information Act, the legal bases relative to Article 10 of the GDPR are supplemented by two further applicable legal bases. Under Section 2 (2) of the Information Act, in case the data processing falls within the scope of the GDPR, Section 5 (7) of the Information Act must also be applied, which provides that: "As regards the processing of personal data from the criminal records, the provisions on the processing of sensitive data shall apply unless an act, an international treaty or a binding legislation of the European Union provides otherwise." These additional legal bases are:

the vital interests of the data subject or of another person, or

the processing relates to data which are manifestly made public by the data subject

These legal bases may be applied in addition to the legal bases listed in Article 9(2) of the GDPR.

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: December 2024*

Yes.

A minor within the meaning of data privacy laws is a person below the age of 16.

## In what circumstances do these special requirements apply?

*Last review date: December 2024*

In the context of information society services (e.g., a commercial website) only if processing is based on consent

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: December 2024*

consent must be given or authorized by the parent/ guardian of the minor

other

privacy information should be provided in plain clear language that minors can understand

data processors must - considering the available technology - make reasonable efforts to check that the consent given is in line with the law

when relying on the legal basis of legitimate interest, the interests or fundamental rights and freedoms of children must be taken into account with particular gravity

specific protection must be applied when using the personal data of children for the purposes of marketing or creating personality or user profiles and the collection of such personal data when using services offered directly to a child

the consent of the parent / guardian may not be necessary in the context of preventive or counselling services offered directly to a child

the child should be able to exercise the rights of the data subject, especially the "right to be forgotten" notwithstanding the fact that they are no longer a child

children cannot be subject to a decision, which may include a measure, evaluating personal aspects relating to them which is based solely on automated processing, and which produces legal effects concerning them or similarly significantly affects them

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: December 2024*

the identity and the contact details of the controller and, where applicable, of the controller's representative

the contact details of the data protection officer, where applicable

the purposes of the processing for which the personal data is intended

the legal basis for the processing

the categories of personal data concerned

the source from which the personal data originates and, if applicable, whether it came from publicly accessible sources

the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground

the recipients or categories of recipients of the personal data, if any

information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available

the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.

the existence of the right to withdraw consent if processing is based on consent

the right to lodge a complaint with a supervisory authority

whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

if applicable, information regarding automated decision making, including profiling

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: December 2024*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

right to access the data subject's own personal data

right to rectify/correct the data subject's own personal data where inaccurate or incomplete

right to erasure of personal data

right to restrict data processing

right to data portability

right to object to the processing of personal data

right to withdraw consent

other: e.g., right to claim compensation for damages or to request a cease and desist order

## Are there accountability and governance requirements?

*Last review date: December 2024*

Yes.

There are accountability and governance requirements to:

take privacy by default and design measures for all processing of personal data

perform and document data protection impact assessments (DPIAs) for high-risk processing:

The NAIH issued a blacklist (available in English [here](http://naih.hu/list-of-processing-operations-subject-to-dpia-35-4--gdpr.html)) on those data processing activities, which most likely constitute high-risk data processing activities and are subject to the DPIA requirement.

maintain a record of processing activities

implement appropriate measures to comply with data privacy and cybersecurity

demonstrate compliance with data privacy and cybersecurity

identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

provide training to employees

audit or supervise data processors

appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

other

Implement the appropriate technical and organizational measures (which, based on the NAIH's practice, must include the implementation of internal policies).

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: December 2024*

Yes.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

Yes.

If yes, under what circumstances?

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 which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

the core activities of the controller or the processor consist of processing on a large scale of special categories of data

the organization employs more than a certain number of individuals in the jurisdiction

other

In cases where an entity falls under the scope of the NIS 2 Directive (e.g. the organization qualifies at least as a medium-sized enterprise and is of a type referred to in the NIS 2 Directive) and provides services specified in Section 1 (b) Article 26 of the NIS 2 Directive, it is mandatory to appoint a representative, if the entity offers services within the EU, but is not established in the EU.

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: December 2024*

Yes.

If yes, what are these requirements?

The DPO must have the ability to fulfil the tasks of the controller or processor pursuant to the provisions of the GDPR, as stated in Section 25/M (1) of the Information Act.

The DPO must keep confidential any personal data, classified information, secrets protected by law and secrets obtained in the course of professional activities the DPO may have learnt in carrying out their activities, as well as any other data, fact or circumstance that their employer data controller or data processor is not required by law to make available to the public during the term of their employment and after the termination thereof.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: December 2024*

No.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: December 2024*

Yes.

The obligations are as follows:

controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

controllers must only use processors subject to a written agreement that complies with specific requirements

other

If the controller is a credit institution under Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (“**Credit Institutions Act**”) and outsources an activity connected to financial services and financial auxiliary services as well as those statutory activities prescribed by law that relate to the processing or storage of data, the controller must notify the Hungarian National Bank (in *Hungarian: Magyar Nemzeti Bank,* “**MNB**”) ([www.mnb.hu](http://www.mnb.hu/)), within two business days after signing the outsourcing agreement, about the fact and duration of outsourcing, as well as the name and registered seat/address of the processor. The outsourcing agreement (i.e., the written engagement of the processor) must contain:

provisions demonstrating compliance with data protection regulations;

the outsourcing service provider’s consent for the supervision of the outsourced activity by the credit institution’s internal control department, its data protection officer or external auditor, and for any on-site or off-site inspections performed by the MNB;

the outsourcing service provider’s responsibility to conduct the activity to an appropriate quality standard and a clause allowing the credit institution’s immediate cancellation of the contract in the event of the outsourcing service provider’s repeated or serious breach of the contract;

the detailed quality service level requirements expected from the outsourcing service provider; and

the rules to be applied in order to avoid insider trading on the part of the outsourcing service provider.

If the controller is an insurance or reinsurance company under Act LXXXVIII of 2014 on the Business of Insurance (the “**Insurance Act**”) and prepares to outsource an activity or function that qualifies as a key activity or function under the Insurance Act, the controller must notify the MNB, five days before the outsourcing agreement is scheduled to take effect, about the fact and duration of outsourcing as well as the name and registered address of the processor. This is also applicable to any changes in the outsourcing agreement regarding key activities or functions. Key functions and activities may not be outsourced, where such outsourcing arrangement (i.e., the engagement of the processor):

is likely to impact the insurance or reinsurance company’s ability to meet its commitments stemming from insurance contracts:

in jeopardizing the system of governance,

by way of increasing operational risks;

prevents the Authority in carrying out its duties; or

is likely to jeopardize the interests of clients.

If the controller is an entity subject to the NIS 2 Directive, the controller must aim to protect network and information systems and the physical environment of those systems with incidents with an all-hazards approach, which includes supply chain security and the security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

In cases where an entity subject to the Cybersecurity Act uses a contractor for the establishment, operation, maintenance or repair of an electronic information system, the contractor (i.e. the data processor) must also meet the basic requirements provided in the Cybersecurity Act. Therefore, the contractor must ensure the security of its electronic information systems and their physical environment in a manner proportionate to the extent of the damage caused by cyber threats.

This protection must include:

the information security management system;

the identification and management of risks to electronic information systems;

the application of administrative, logical and physical measures to mitigate risks, appropriate to the level of security to be defined for each system in the organization's risk analysis;

the prevention, detection, management and mitigation of security incidents;

ensuring business continuity; and

the acquisition, development and operation of electronic information systems and the software and hardware products used by them.

The head of the entity concerned must ensure that these basic requirements are provided for in a contract.

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: December 2024*

Yes.

The following provisions apply directly to processors:

Art. 28, 29, 30 para. 2, 31, 32, 33 para. 2, 37 et seq., 44 et seq. GDPR.

With respect to entities governed by the Credit Institutions Act, the processor (i.e., the outsourcing service provider) must meet — to a degree corresponding to the risk — the personnel, infrastructure and security requirements concerning the outsourced activities that are prescribed by law for credit institutions [Section 68 (2) of the Credit Institutions Act].

Regarding insurers and reinsurers governed by the Insurance Act, the controller (i.e., the insurance or reinsurance company) is responsible for ascertaining that the processor (i.e., the outsourcing service provider) is performing the activity in compliance with the relevant legislation and with due care and attention. If the processor performs the outsourced functions in serious breach of the outsourcing contract, or, in spite of a warning, continues to perform those functions in violation of the law or in breach of the outsourcing contract, the controller must terminate the outsourcing contract with immediate effect [Section 91 (2) of the Insurance Act].

With respect to entities subject to the Cybersecurity Act, the head of the relevant entity is responsible for ensuring that the basic requirements required by the Cybersecurity Act are provided for in a contract between the controller and contractors [Section 6 (5) of the Cybersecurity Act].

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: December 2024*

Yes.

Third country is not defined in the GDPR, but means countries outside of the European Economic Area.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

approved adequate/whitelisted jurisdictions

to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and cybersecurity authority (e.g., EU-US Data Privacy Framework)

approved standard contractual clauses

binding corporate rules

derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims

other solutions

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

ad-hoc contracts approved by the data protection authority

Note: regarding "holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and security authority," the certification may be received or the code of conduct approved only in line with the GDPR. In light of the rulings of the Court of Justice of the European Union, the approval by a data protection authority of a country that is not a member of the EU does not necessarily safeguard the rights, freedoms and interests of the data subjects (decision in case no. C-311/18; "Schrems II decision," invalidating the EU/US Privacy Shield Framework as a tool for personal data transfer to third countries).

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: December 2024*

Yes.

On 17 February 2017, the NAIH released cookie guidance. The guidance says that the use of user-input cookies, authentication cookies, user-centric security cookies, multimedia player session cookies, load balancing session cookies, and user interface customization cookies does not require any consent. However, if this cookie consent exemption does not apply to the type of cookie used - such as in connection with the use of third party cookies or tracking cookies - then the website operator must secure the user's voluntary consent to the use of a cookie.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: December 2024*

Yes.

**Email marketing**

prior opt-in consent

prior existing business relationship (and subject to other requirements) with opt-out consent (applicable only to direct marketing that is not addressed to a natural person)

**Telephone marketing**

prior opt-in consent

prior existing business relationship (and subject to other requirements) with opt-out consent (applicable only to direct marketing that is not addressed to a natural person)

**SMS/text message marketing**

prior opt-in consent

prior existing business relationship (and subject to other requirements) with opt-out consent (applicable only to direct marketing that is not addressed to a natural person)

**Postal marketing**

prior opt-in consent

opt-out or implied consent (subject to compliance with specific requirements)

**Online behavioral advertising targeting/ social media targeting/ad personalization marketing**

prior opt-in consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: December 2024*

Yes.

The potential legal bases for data processing in the employment context are:

consent (please see restrictions below)

performance of contract

compliance with legal obligation

protection of vital interest

public interest

legitimate interest

## Can consent be validly obtained in the employment context?

*Last review date: December 2024*

Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

Consent can validly obtained in employment context if the voluntary nature of the consent can be proven; otherwise, the validity of consent is likely to be challenged based on the NAIH's practice to date.

Furthermore, pursuant to recital 43 GDPR, "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller", which could be the case in the employment relationship.

On 15 November 2016, the NAIH released comprehensive guidance about the basic requirements of data processing in the employment context. The guidance confirms that Hungarian employers may not rely on consent as a legal basis for the processing of employee data - unless the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment. The NAIH holds the view that this is only rarely the case in the employment context, due to the subordinate relationship among the employer and the employee. The employer therefore generally must rely on a legal basis other than employees' consent to process employee data in the employment context.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide cybersecurity and other data-related legislation.*

Yes

The NAIH published a relevant decision regarding the use of artificial intelligence based technology and imposed the largest fine to date in Hungary, which was a fine of HUF 250,000,000 (approximately EUR 612,000). The decision was published in [NAIH’s annual report for 2022](https://naih.hu/hirek/540-elerheto-a-hatosag-2022-evi-beszamoloja) (and the text of the decision is publicly available [here](https://naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei)). Details of that decision can be found in the Artificial Intelligence, Profiling and Automated Decision Making chapter.

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: December 2024*

Yes.

The restrictions or requirements are as follows:

qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

right to information / transparency requirement

other

Data subjects have a right to request human review of the automated decision making if the decision produces legal effects concerning them or that similarly significantly affect them.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: December 2024*

Yes.

The exceptions are as follows:

If the decision:

is necessary for entering into, or performance of, a contract between the data subject and a data controller

is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or

is based on the data subject's explicit consent

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide cybersecurity and other data-related legislation.*

Yes

The NAIH published a relevant decision in 2022 regarding the use of artificial intelligence based technology in relation to the bank’s data processing regarding the recording of customer service calls and imposed the largest fine to date in Hungary, of HUF 250,000,000 (approximately EUR 612,000).

The bank recorded customer service calls automatically and analyzed the audio recordings with technology based on artificial intelligence. The bank used the results of such analyses to decide on which customers it shall call back. During such analyses, the bank also assessed the data subjects’ emotional state.

The NAIH held that the bank:

did not weigh, in its legitimate interest balancing test relative to the analysis of audio records, the significant risks to fundamental rights that the data processing might impose; therefore, the legitimate interest balancing test was invalid and the data processing did not have a proper legal basis;

did not include information, in its privacy notice, about the analysis of audio records; therefore, the bank did not notify the data subjects about the data processing and did not enable the data subjects to object to the data processing; and

did not take into consideration that it must limit the data processing to the necessary extent relative to its employees and did not provide proper notification about the data processing to its employees.

In addition to the above, the NAIH highlighted that artificial intelligence is generally difficult to understand and follow, due to the way it operates; therefore, the use of artificial intelligence requires particular care during data processing.

The decision was published in [NAIH’s annual report for 2022](https://naih.hu/hirek/540-elerheto-a-hatosag-2022-evi-beszamoloja) (and the text of the decision is publicly available from [here](https://naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei)).

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: December 2024*

Enforcement activity against AI user(s)/deployer(s)

Enforcement activity under existing privacy law

Enforcement activity by data or cyber regulator

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide cybersecurity and other data-related legislation.*

Yes, laws in force

The EU chapter contains information on the relevant EU legislation.

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: December 2024*

Yes

Case no. NAIH-7731-2/2022.

In this case the NAIH stated that on the date of the merger, the rights and obligations of the merging company in relation to data processing operations are also transferred to the acquiring company, including contracts with users and the related data processing operations. In the opinion of the NAIH, in such a case the personal data processed shall be deemed to have been obtained by the legal successor directly from the data subjects.

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: December 2024*

No

## If so, how would any regulatory fines be calculated?

*Last review date: December 2024*

N/A

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: December 2024*

Yes

## If so, how would any regulatory fines be calculated?

*Last review date: December 2024*

Unclear

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: December 2024*

Yes.

general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

obligation to take specific security measures e.g., encryption

requirement to undertake third party due diligence (security assessment of third party providers)

reasonable security controls

encryption

Although not a strict legal requirement, encryption is considered by the GDPR as an appropriate technical and organizational measure. In practice, the authorities expect encryption to be used unless specific circumstances justify its absence.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: December 2024*

network information security requirements (broader than telecommunications)

financial services requirements

telecommunication requirements

providers of critical infrastructure

digital or connected (IoT) products

other

The relevant general obligations of the [EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679) and the Information Act are applicable to all controllers and processors of personal data.

In addition, Hungarian laws and regulations — together with certain EU laws — impose further data security related obligations on the following economic actors:

Various types of financial service providers (e.g., financial institutions, insurance companies and investment firms);

Providers of online marketplaces, location tool services and cloud computing services (in light of the Country-of-Origin principle);

Service providers involved in the operation of critical infrastructures and/or the provision of essential services; and

Manufacturers of IoT devices, which are elements or groups of elements of a network or information system that interact with the environment through signal conversion.

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

financial services

telecommunications

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: December 2024*

Yes.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Incident" means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

## Controllers/Owners have to notify:

*Last review date: December 2024*

**Data protection authorities**

in case of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

without undue delay and, where feasible, not later than 72 hours after having become aware of it

**Cybersecurity authorities**

without undue delay

Due to the implementation of the NIS 2 Directive in Hungarian law, in line with Section 77 of Government Decree 418/2024 (XII. 23.), the following apply:

an early warning must be reported without undue delay and in any event within 24 hours;

early warnings must be followed by an incident notification, without undue delay and in any event within 72 hours.

**Affected individuals**

if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects, the controller shall communicate the personal data breach to the data subject without undue delay (GDPR Art. 34 Section 1); unless any of the following conditions are met:

the controller has implemented technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize;

it would involve disproportionate effort.

**Other**

If the (direct and individual) communication to the data subjects would involve disproportionate effort, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (compared to direct communication) without undue delay [GDPR Art. 34 Section 3 Point c)].

## Processors/Agents have to notify:

*Last review date: December 2024*

Controller/ owner

in case of a personal data breach irrespective of a risk to the rights and freedoms of the data subjects

without undue delay after becoming aware of it

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: December 2024*

Yes.

cybersecurity authorities

financial services requirements

telecommunication requirements

providers of critical infrastructure

other

Providers of services subject to notification requirement (e.g., operators of online marketplaces, location tool services and cloud computing services) pursuant to the E-Commerce Act.

**Details regarding the identified data security breach notification requirements**

Security incident notification requirements for entities subject to the Cybersecurity Act are determined by 418/2024 (XII.23.) Government Decree. The Cybersecurity Act and its implementing government decree set different obligations on organizations of the public administration, on state owned entities and other relevant entities.

Entities under the scope of the Cybersecurity Act must submit an early warning to the NBSZ without undue delay and in any event within 24 hours. This must be followed by an incident notification without undue delay and in any event within 72 hours.

Sector-specific data breach notification requirements in Hungary relative to electronic communications:

The providers of public electronic communication services in Hungary must file a notification if the personal data of telecom services subscribers is breached. The notification must be provided to the National Media and Infocommunications Authority ("**NMHH**") by the public electronic communication services provider via NMHH's online platform ("**Adatkapu**").

Section 156 (2) of the Electronic Communications Act defines a “breach of the subscribers' personal data” as a breach of security leading to the accidental or unlawful use or processing of personal data, meaning, in particular, the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service. No exceptions apply to the breach notification obligation of service providers; any breach event must be reported promptly, but within 24 hours at the latest, to the NMHH.

Sections 156 (2)-(8) of the Electronic Communications Act establish a personal data breach notification obligation for providers of public electronic communication services to the NMHH. NMHH Decree No. 4/2012 (I.24.) establishes the details of the data breach notification obligation.

If the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or of other private individuals, the provider of electronic communications services must notify the concerned data subjects without undue delay, but within 24 hours at the latest. However, notification to a subscriber or private individual concerned is not required if the telecoms services provider has demonstrated to the satisfaction of the NMHH that it has implemented appropriate technological protection measures and that those measures were applied to the data affected by the security breach. Such technological protection measures must be capable of rendering the data unintelligible to any person who is not authorized to access it.

If the service provider has not notified the subscriber or private individual of the personal data breach, the NMHH, having evaluated the likely adverse effects of the breach and following consultation with the NAIH, may order the service provider to do so.

If a personal data breach occurs, firstly, the telecoms services provider must , notify the NMHH concerning that breach without undue delay, but within 24 hours at the latest. If the telecom services provider does not possess some of the data required to be included in that notification, the service provider must commence an internal investigation, and, within 24 hours from the occurrence of the breach, notify the NMHH (the first notification). Subsequently, the telecoms service provider must gather the information necessary for the second notification and, if necessary, update the content of the first notification which must be submitted without undue delay, but within 72 hours from the first notification (the second notification).

If the telecoms service provider cannot submit all of the information required to be submitted in the second notification, it must provide the information available at that point within 72 hours of the breach, explaining to the NMHH why it could not submit the remaining required information within the 72-hour timeframe. The telecoms service provider must inform the NMHH monthly about the findings arising from the provider's internal investigation in the past month, until the investigation is closed or the reasons due to which the data breach occurred have been addressed.

A public electronic communications service provider has the following reporting obligations in case of network outages:

without undue delay, to the Government Incident Response Team, about any security incident affecting their electronic communications networks, including any threat of which they are aware, and which are likely to result in potentially unfavorable changes or any previously unknown situations in the Electronic Communication Networks or Electronic Communication Services, or in consequence of which the confidentiality, integrity, authenticity, functionality or availability of information carried via the Electronic Communication Networks or Electronic Communication Services is either lost or compromised; and

without delay, to the General Informatics and Electronic Communication Inspectorate of the NMHH, via an electronic form provided by the Office of NMHH regarding any network security incidents affecting the operation of the network and of the services.

If the controller is a payment service provider and the personal data breach is a major operational or security incident under Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (“Payment Services Act”), the controller must notify the Hungarian National Bank without undue delay [Section 55/B (1) of the Payment Services Act)]. This obligation of the controller does not affect its reporting obligation to NAIH based on the GDPR. If the major operational or security incident has or may have an impact on the financial interests of its payment service users, the payment service provider must, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

Financial entities in Hungary that are under the scope of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("DORA") must report any unplanned event that compromises the security of the network and information systems, and has an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity ("major ICT-related incident") to the relevant competent authority referred to in DORA.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: December 2024*

Yes.

a)   data localization / data residency laws that mandate retention of personal data or a copy thereof in the local jurisdiction (include whether copies or the original data may be also be stored outside of the jurisdiction):

Under Act CL of 2017 on the Rules of Taxation, originals of accounting documents and books and records, including records stored in electronic media, must be kept in a place registered with the Hungarian National Tax and Customs Administration ("**NAV**") for that period and extent specified in the registration notice. Documents may be taken to another place for the purpose of bookkeeping and processing for the duration required, but the original documents must be presented to the NAV within three working days at its request.

b)   other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

The following laws merit mention because the information and data they regulate may qualify as personal data of natural persons:

Pursuant to Hungarian Act CLV of 2009 on the Protection of Classified Information, access to classified information may be granted only to individuals with a personnel security clearance having an acknowledgement of secrecy, with the rights of disposal defined in the user license. The user license grants the right for example to hold classified information, transfer it further outside an entity or organization, and authorizes access to classified information to foreign persons or foreign bodies.

Pursuant to Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises, bank secrets must be kept secret without time limitation and may not be disclosed - except, as to bank secrets in the course of outsourcing as specified in the Act - without the consent of the owner of the secret.

Pursuant to Act LXXXVIII of 2014 on the Business of Insurance, insurance secrets must be kept secret without time limitation and may not be disclosed - except, as to insurance secrets in the course of outsourcing as specified in the Act - without the consent of the owner of the secret.

For Law Enforcement, National Security and Defense purposes, Act CVIII of 2001 on the Electronic Commerce and on Information Society Services ("**E-Commerce Act**") specifies the data retention period that applies to the application service providers of services featuring encrypted communication, where metadata in connection with transmissions and communications executed through such application is retained.

For Law Enforcement, National Security and Defense purposes, Act C of 2003 on Electronic Communications ("**Electronic Communications Act**") contains specific mandatory requirements concerning permitted data retention purposes.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: December 2024*

Obligation for public sector organizations to share or make accessible non-personal data

Any person or body performing statutory state or municipal government functions or performing other public duties provided for by the relevant legislation must allow free access to any person to the public information and information of public interest they have on file, under the provisions of the Information Act.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: December 2024*

Obligation to share data on request

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.