Global Data and Cyber Handbook - Hungary

Regulators, Enforcement Priorities and Penalties

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

# 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

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.