Act CXXV of 1995
on national security services

The National Assembly, with a view to protecting the independence and lawful order of Hungary, adopts the following Act on the constitutional operation of the national security services:

Organisation and legal status of national security services

Section 1 The national security services of Hungary shall be the following:
a) the Information Office,
b) the Constitution Protection Office,
c) the Military National Security Service,
d) the Special Service for National Security, and
e) the Counter-Terrorism Information and Criminal Analysis Centre
(hereinafter jointly "national security services").

Section 2 (1) The Information Office, the Constitution Protection Office, the Special Service for National Security, the Counter-Terrorism Information and Criminal Analysis Centre (hereinafter jointly "civilian national security services") and the Military National Security Service shall be budgetary organs under the direction of the Government with territorial competence over the whole territory of the country that manage their affairs autonomously.

(2) In accordance with directional decisions by the Government, national security services may establish local or regional organs to perform the tasks set out in this Act.

Tasks of national security services

Section 3

Section 4 The Information Office

a) shall obtain, analyse, evaluate and transfer information that are necessary for governmental decisions and relate to, or originate from, foreign countries and are usable in the interest of the security of the nation; furthermore, shall perform activities for furthering the interests of Hungary;

b) shall detect foreign secret service endeavours and activities interfering with, or threatening, the sovereignty or the political, economic or other significant interests of Hungary;

c) shall gather information about foreign organised crime threatening national security and, in particular, about terrorist organisations, illegal drug or arms trafficking, as well as about the illegal international traffic of weapons of mass destruction and their components and of the materials and tools necessary for their production;

d) shall detect foreign intentions and acts aimed at threatening the security of the economy, and the financial standing, of the country;

e) shall participate in the detection and prevention of illegal trafficking in internationally controlled products and technologies;

f) shall provide security protection for Hungarian organs (institutions) and facilities abroad that are significant for governmental activities;

g) shall provide national security protection for persons falling within its material competence, and operational protection for its facilities; and shall perform the national security vetting of its personnel and other persons falling within its material competence;

h) shall perform cryptographic supervision and classification of encryption methods and algorithms used for the protection of classified data and of devices used for encryption outside the national borders; furthermore, shall generate encryption keys;

i) shall, regarding its own personnel, perform internal security and crime prevention control duties and monitor impeccable lifestyle;

j) may carry out additional checks, as set out in the Act on procurement for defence and security purposes, regarding its own qualified procurements.

Section 5 The Constitution Protection Office

a) shall detect and ward off foreign secret service endeavours and activities interfering with, or threatening, the sovereignty or the political, economic, security or other significant interests of Hungary;

b) shall detect and ward off covert endeavours to change or disturb the lawful order of Hungary by illegitimate means;

c)

d) shall detect and ward off covert endeavours threatening the economic, scientific and technical, and financial security of Hungary, as well as illegal drug and arms trafficking;

e) shall provide security protection for organs (institutions) and facilities that are significant for central state power and governmental activities;

f) shall provide national security protection for persons falling within its material competence, and shall perform the national security vetting of persons subject to national security vetting other than the persons falling within the material competence of the Military National Security Service, the Special Service for National Security or the Information Office;

g) shall carry out the screening of persons applying for a document certifying permanent resident status, seeking refugee status or applying for Hungarian citizenship, and in connection with the protection of the sovereignty of the State and the lawful order, of persons having submitted an application for visa; as well as the related tasks;

h) shall detect, until an investigation is ordered, the following criminal offences:

ha) under Act IV of 1978 on the Criminal Code (hereinafter "Act IV of 1978"), as in force until 30 June 2013, criminal offences against the State (Chapter X of Act IV of 1978), crimes against humanity (Chapter XI of Act IV of 1978), and within its area of responsibility, desertion abroad (section 343 of Act IV of 1978), mutiny (section 352 of Act IV of 1978) and compromising combat readiness (section 363 of Act IV of 1978), and

hb) under Act C of 2012 on the Criminal Code (hereinafter the "Criminal Code"), crimes against humanity (Chapter XIII of the Criminal Code), war crimes (Chapter XIV of the Criminal Code), criminal offences against the State (Chapter XXIV of the Criminal Code) and within its area of responsibility, desertion (section 434 of the Criminal Code), mutiny (section 442 of the Criminal Code) and endangering an increase in the state of readiness (section 454 of the Criminal Code);

i)

j) shall obtain information regarding the following criminal offences:

ja) under Act IV of 1978, as in force until 30 June 2013, violence against a member of a national, ethnic, racial or religious group (section 174/B of Act IV of 1978), misuse of data classified as top secret or secret (section 221 of Act IV of 1978), causing public danger (section 259 of Act IV of 1978), violation of an international economic restriction (section 261/A of Act IV of 1978), unlawful seizure of an aircraft, rail vehicle, watercraft or road vehicle used for public transport or suitable for the transport of bulk goods (section 262 of Act IV of 1978), agitation against a community (section 269 of Act IV of 1978), fearmongering (section 270 of Act IV of 1978) and threatening with public danger (section 270/A of Act IV of 1978), and

jb) violence against a member of a community (section 216 of the Criminal Code), misuse of classified data (section 265 of the Criminal Code), unlawful seizure of a vehicle (section 320 of the Criminal Code), causing public danger (section 322 of the Criminal Code), violation of an international economic restriction (section 327 of the Criminal Code), failure to report a violation of an international economic restriction (section 328 of the Criminal Code), incitement against a community (section 332 of the Criminal Code), fearmongering (section 337 of the Criminal Code) and threatening with public danger (section 338 of the Criminal Code);

k) shall participate in the detection, prevention and prohibition of the illegal traffic of internationally controlled products and technologies, and in the control of their legal traffic;

l) shall participate in the detection, prevention and prohibition of the illegal traffic of military equipment and services, and in the control of their legal traffic;

m) shall, at the request of the National Security Authority, perform the audit of economic operators falling within its competence;

n) shall perform preliminary qualification and qualification related to procurement procedures under the Act on procurement for defence and security purposes; furthermore, it may carry out the necessary additional checks regarding its own qualified procurements;

o) shall check persons seeking permission to issue a card under the Act on the uniform electronic card issuing framework, and shall perform the related tasks;

p) shall detect and ward off covert activities by persons or groups who threaten the national security of Hungary, are connected to an application under point *g)*, enter or stay in Hungary unlawfully, or facilitate such entering or staying, and threaten the national security of the country by doing so.

Section 6 The Military National Security Service

a) shall expose endeavours indicating an intention to attack or influence Hungary and shall further the interests of Hungary abroad in accordance with its own system of tasks;

b) shall detect and ward off foreign secret service endeavours and activities interfering with, or threatening, the sovereignty or the national defence interests of Hungary;

c) shall obtain, analyse and transfer military policy, defence industry and military information originating from a foreign country that are necessary for governmental decisions and that are related to the military elements of security policy;

d) shall, within the area of its responsibility, detect and ward off covert endeavours to change or disturb the lawful order of Hungary by illegitimate means;

e) shall gather information affecting its tasks about crisis areas and endeavours and activities threatening the corps of the Hungarian Defence Forces and their personnel in operational areas; and shall take part in the national security protection, preparation and support of the Hungarian Defence Forces deployed in operational areas;

f) shall provide information necessary for the defence and strategic and operational planning of the ministry lead by the Minister responsible for national defence and of the Hungarian Defence Forces Command; and shall operate the single military reconnaissance system of Hungary;

g) shall gather information about cyber activities and cyber organisations threatening national defence interests; shall carry out, within the framework of the law, the tasks of the national defence sector relating to electronic information security; and shall provide information necessary for the tasks relating to information assurance planning of the ministry led by the Minister responsible for national defence and of the Hungarian Defence Forces Command; and shall, by using its operational capabilities within the cyberspace, provide national security-related protection to national defence interests, and support to the cyber defence and cyber operations of the Hungarian Defence Forces;

h) shall gather information about terrorist organisations threatening national security; and shall, with regard to national defence organisations, detect and ward off endeavours of foreign powers, persons and organisations to commit a terrorist attack;

i) shall gather information about illegal arms trafficking threatening national security and organised crime threatening the security of the ministry led by the Minister responsible for national defence and of the Hungarian Defence Forces, with a focus on illegal drugs and arms trafficking;

j) shall participate in detection, prevention and prohibition of the illegal traffic of internationally controlled products and technologies, and of military equipment and services, as well as in the control of their legal traffic;

k) shall, within its competence, provide security protection for military organs and facilities (institutions), as well as governmental and military headquarters, which are significant for governmental activities;

l) shall detect, until an investigation is ordered, the following crimes within its area of responsibility:

la) under Act IV of 1978, as in force until 30 June 2013, criminal offences against the State (Chapter X of Act IV of 1978), crimes against humanity (Chapter XI of Act IV of 1978), desertion abroad (section 343 of Act IV of 1978), mutiny (section 352 of Act IV of 1978) and compromising combat readiness (section 363 of Act IV of 1978), and

lb) crimes against humanity (Chapter XIII of the Criminal Code), war crimes (Chapter XIV of the Criminal Code), criminal offences against the State (Chapter XXIV of the Criminal Code), desertion (section 434 of the Criminal Code), mutiny (section 442 of the Criminal Code) and endangering an increase in the state of readiness (section 454 of the Criminal Code);

m) shall detect the following criminal offences within its area of responsibility:

ma) terrorist act under Act IV of 1978, as in force until 30 June 2013 (section 261 of Act IV of 1978), and

mb) terrorist act (sections 314 to 316/A of the Criminal Code), failure to report a terrorist act (section 317 of the Criminal Code) and terrorism financing (sections 318 to 318/A of the Criminal Code) or incitement to war (section 331 of the Criminal Code);

n) shall gather information about the following criminal offences within its area of responsibility:

na) under Act IV of 1978, as in force until 30 June 2013, violence against a member of a national, ethnic, racial or religious group (section 174/B of Act IV of 1978), misuse of data classified as top secret or secret (section 221 of Act IV of 1978), causing public danger (section 259 of Act IV of 1978), violation of an obligation under international law (section 261/A of Act IV of 1978), unlawful seizure of an aircraft, rail vehicle, watercraft or road vehicle used for public transport or suitable for the transport of bulk goods (section 262 of Act IV of 1978), agitation against a community (section 269 of Act IV of 1978), fearmongering (section 270 of Act IV of 1978), threatening with public danger (section 270/A of Act IV of 1978) and abuse of military products or services, or of dual-use products (section 263/B of Act IV of 1978), and

nb) violence against a member of a community (section 216 of the Criminal Code), misuse of classified data (section 265 of the Criminal Code), unlawful seizure of a vehicle (section 320 of the Criminal Code), causing public danger (section 322 of the Criminal Code), violation of an international economic restriction (section 327 of the Criminal Code), failure to report a violation of an international economic restriction (section 328 of the Criminal Code), abuse of military products or services (section 329 of the Criminal Code), abuse of dual-use products (section 330 of the Criminal Code), incitement against a community

(section 332 of the Criminal Code), fearmongering (section 337 of the Criminal Code) and threatening with public danger (section 338 of the Criminal Code);

moreover, shall detect criminal offences threatening the performance of the tasks, under the law, of national defence organisations;

o) shall perform national security tasks related to defence industrial research, development, production and trade conducted by national defence organisations;

p) shall, at the request of the National Security Authority, perform the audit of economic operators falling within its competence;

q) shall perform the preliminary qualification and qualification related to procurement procedures under the Act on procurement for defence and security purposes; furthermore, it may carry out the necessary additional checks regarding its own qualified procurements

r) shall perform the tasks relating to the national security protection, and the national security vetting, of persons within its competence;

s) shall perform internal security and crime prevention control duties regarding its personnel within its competence;

t) shall perform the tasks set out in points *a)* to *r)* concerning companies specified in a decree by the Minister responsible for national defence carrying out activities related to national defence interests.

Section 7 (1) The Military National Security Service shall analyse and evaluate information concerning the military elements of national security detected during the exercise of its functions specified in section 6 *a)* to *g)*, *i)* to *l)*, *n)* to *s)* within its area of responsibility; and shall keep informed thereof the executives vested with the relevant functions and powers of the ministry led by the Minister responsible for national defence, the commanders and executives of the Hungarian Defence Forces vested with the relevant functions and powers, the commander of the Hungarian Defence Forces, the Minister responsible for national defence and the Commander in Chief of the Hungarian Defence Forces.

(2) The Military National Security Service shall provide, without delay and without performing analysis or evaluation, the Counter-Terrorism Information and Criminal Analysis Centre with the information obtained in the course of the performance of its tasks under section 6 *h)* and *m)*.

(3) Within its area of responsibility, the Military National Security Service shall autonomously perform its tasks necessary for the fulfilment of the obligations of Hungary under international treaties or assigned under sections 9 *b)* and 11 (2) *b)* and *i)*.

Section 8 (1) The Special Service for National Security

a) shall, within the framework of laws, by using its means and methods and upon a written request, provide services for the implementation of secret information gathering and the use of covert means as specified in the Act on the Code of Criminal Procedure (hereinafter "covert means") to the organs authorised to engage in secret information gathering and to use covert means;

b) shall, according to the needs of the organs authorised to engage in secret information gathering or to use covert means, provide the specific technical tools and materials required for such activities;

c) shall ensure special telecommunications connectivity to users specified by the Government;

d) shall provide administrative supervision in relation to the protection of security documents;

e) shall perform the tasks of an expert or, as set out in a specific law, of a judicial expert;

f) shall provide operational protection for its facilities and conduct the national security vetting of its personnel and other persons within its competence;

g) may carry out additional checks regarding its own qualified procurements under the Act on procurement for defence and security purposes,

h) shall, at a request from the prosecution service, an investigating authority, an organ conducting a preparatory proceeding, an organ authorised to engage in secret information gathering, or a national security service, participate in requesting data that may be processed lawfully by the requesting party,

i) shall perform electronic information security-related tasks as provided for by law,

j) shall perform tasks of an authority related to the protection of classified data and to facility industrial security, as provided for by law.

(2) The Special Service for National Security shall not be engaged in any governmental information activities.

(3) The Special Service for National Security may, on its own initiative, carry out the activities, and use the means and methods, specified in section 54 (1) for the performance of its tasks set out in paragraph (1) *a)* to *f)* and carry out the activities specified in section 54 (1) *f)*, *g)* and *j)* for the performance of its tasks set out in paragraph (1) *i)*.

(4) The Special Service for National Security shall not use the means and methods of secret information gathering specified in section 56 on its own initiative with the exception of the performance of the tasks under paragraph (1) *f)*.

(5) With the exception of the performance of the activities of a judicial expert as set out in paragraph (1) *e)*, the Special Service for National Security shall provide its services free of charge.

(6) The Government shall determine the order of cooperation between the organs authorised to engage in secret information gathering or to use covert means, and the Special Service for National Security.

(7) With the exception of the provisions of section 6 *g)* and military cyberspace operations, relating to its tasks concerning information security, the Special Service for National Security shall

a) provide protection against cyber threats and attacks to organs falling within the scope of the Act on electronic information security of State and local government organs in accordance with the rules on material competence set out therein,

b) direct, with the exception of the national defence sector, preparation for cyber threats and the related security tasks,

c) monitor the traffic on electronic communications networks, without intercepting any communication, and detect cyber threats and attacks,

d) perform and initiate the measures necessary to interrupt cyber attacks.

(8) The measure under paragraph (7) *d)* can only be performed based on the relevant decision by the person designated by the Government. After an attack is interrupted, the possible measures necessary for increasing security, and the necessity of further decisions relating to the protection of the country, shall be examined.

(9) A measure under paragraph (7) *d)*

a) shall be proportional to the harm caused or the direct threat and shall be imposed to the necessary extent; effort shall be made to avoid reaching any result in excess of the interruption of the attack, or causing any harm,

b) shall ensure consistency with national security, national defence, law enforcement and foreign policy interests and efforts.

(10) In case of a significant foreign cyber attack, the Minister responsible for foreign policy shall be informed of the measures taken and their reasons with a view to taking further measures.

Section 8/A (1) The Counter-Terrorism Information and Criminal Analysis Centre shall examine the security and criminal situation in Hungary, and in this framework it

a) shall monitor and shall, using all available data, continuously analyse the national security, criminal and terrorist threat situation in Hungary;

b) shall, upon request, evaluate, by taking into account experience accumulated within the framework of cooperation and coordination, the performance of tasks falling within the functions and powers related to the provision of governmental information of certain cooperating organs;

c) shall continuously monitor information concerning the terrorism situation in Hungary;

d) shall perform coordination activities, by involving the organisations concerned, in a case of direct terrorist threat or regarding high-risk security issues;

e) shall monitor trends, and prepare analyses and studies about new phenomena, concerning the security and criminal situation in Hungary.

(2) With a view to facilitating strategic decision-making related to national security, criminal and terrorist threat issues, the Counter-Terrorism Information and Criminal Analysis Centre

a) shall make proposals to the Ministers directing national security services to determine timely tasks;

b) shall perform governmental information and decision support activities, as well as analysis activities related to security policy and criminal strategy; and shall, for this purpose, specify information needs as regards to cooperating organs;

c) shall make proposals to determine the level of terrorist threat based on an evaluation of information concerning terrorism situation in Hungary;

d) shall assemble, continuously update and send to the cooperating organs the *ad hoc* and periodic information requests specified by the Government as necessary for decision-making;

e) shall perform information activities for the Government, the organisation preparing the national security decisions by the Government and the working group assisting that organisation, by using information available, or being generated, in connection with the information requests;

f) shall, by providing de-identified statistical data resulting from the analysis of data processed by it, assist in governmental decision-making related to security and criminal issues,

in the course of performing governmental information activities.

(3) In the course of support, coordination, analysis and evaluation activities, the Counter-Terrorism Information and Criminal Analysis Centre

a) shall perform analysis, information and coordination activities covering

aa) all information conferred upon cooperating organs, and

ab) data and information processed as part of secret information gathering and using covert means, and a preparatory proceeding or investigation within the meaning of the Act on criminal procedure, that is carried out by the prosecution service and falls within the scope set out in the agreement referred to in section 52/A (3);

b) shall provide feedback to cooperating organs and the prosecution service about the use of their information, and about further tasks and directions of information gathering deriving therefrom;

c) shall manage databases with the aim of performing analysis tasks, supporting cooperating bodies, and supporting the prosecution service in the exercise of its power referred to in point *a) ab)*, to facilitate coordination at a national level;

d) shall operate service provider and support organs performing the gathering and technical processing of information from open sources;

e) shall provide information support to the Government, the organisation preparing national security decisions by the Government and the working group assisting that organisation, by preparing analyses;

f) shall perform analysis, evaluation and coordination activities in cases of national importance affecting multiple organs, as well as in cases specified by the Government, the organisation preparing national security decisions by the Government and the working group assisting that organisation;

g) shall prepare information reports and background and risk analyses related to the national security, terrorist threat and criminal situation in Hungary, to certain elements thereof, and to specific risks and criminal offences, for the cooperating organs with a view to facilitating the lawful, professional and effective performance of tasks falling within the competence of those organs and for the prosecution service with a view to facilitating the lawful, professional and effective performance of tasks specified under point *a) ab*;

h) shall reveal any concurrent secret information gathering, or concurrent use of covert means, by cooperating organs or by cooperating organs and the prosecution service concerning the same criminal offence, person or other subject matter, and any concurrent data processing as regards concurrent investigations and preparatory proceedings regarding the same criminal offence; and shall inform the prosecution office and the cooperating organ concerned of this;

i) in a case where

ia) it suspects that a criminal offence, including an attempt of, or where preparation is punishable under an Act, a preparation for, a criminal offence, occurred, shall, by observing the provisions of section 52/E (2), report the crime to the investigating authority, or the prosecution office, having material and territorial competence over the investigation, shall hand over the data gathered by it, and may, where appropriate, propose the use of covert means;

ib) it obtains information based on which preparatory proceedings under the Act on the Code of Criminal Procedure may be conducted, shall, by observing the provisions of section 52/E (2), initiate preparatory proceedings at the prosecution office, or investigating authority, having relevant territorial and material competence, the police organ performing internal crime prevention and crime detection tasks, or the counter-terrorism police organ; may hand over the data gathered by it, and may, where appropriate, propose the use of covert means;

ic) it obtains information based on which measures may be taken that fall within the competence of national security services or counter-terrorism police organs, may hand over the data gathered by it to the competent national security service or the counter-terrorism police organ for the purpose of initiating such measures; and may, where appropriate, propose the use of covert means;

j) shall monitor the availability of information clarifying or complementing data created in the course of a preparatory proceeding, investigation, or secret information gathering, conducted by a cooperating organ or the prosecution service and used by the Counter-Terrorism Information and Criminal Analysis Centre; if it is processed by the prosecution service or another cooperating organ, the Counter-Terrorism Information and Criminal Analysis Centre shall inform the organs concerned and shall initiate contact;

k) shall monitor the activity of criminal and terrorist organisations, organised crime and terrorist groups, the relationships and connections between these organisations and groups; and by analysing their efforts to conceal their illegally acquired assets or the illegal origin of such assets, and their enterprises serving for these purposes, it shall assist in taking actions against them;

l) shall, upon transferring data processed by it to a cooperating organ, make proposals on the use of the data in a further proceeding falling within the functions and powers of a cooperating organ.

(4) The Counter-Terrorism Information and Criminal Analysis Centre shall perform the tasks of a passenger information unit.

(5) In the case under paragraph (3) *h)*, if one of the organs processing data concurrently is the prosecution service, a police organ performing internal crime prevention and crime detection tasks, the Information Office or the Military National Security Service, then the Counter-Terrorism Information and Criminal Analysis Centre may inform the another cooperating organ about the concurrent data processing only with consent of the Prosecutor General or the director-general of the police organ performing internal crime prevention and crime detection tasks, the Information Office or the Military National Security Service.

(6) Cooperating organs shall inform, within 8 working days, the Minister responsible for direction and the Counter-Terrorism Information and Criminal Analysis Centre about the use of data transferred by the Counter-Terrorism Information and Criminal Analysis Centre and about the acceptance or dismissal of a proposal on the use of data, or of any other indication or initiative, by the Counter-Terrorism Information and Criminal Analysis Centre.

Section 9 National security services

a) shall procure, research and develop technical systems and means necessary for the performance of their tasks and provide professional training related to the use of such means, and for this purpose, may cooperate with each other and with other organs;

b) shall perform the tasks, specified by an Act, in connection with a state of national crisis, a state of emergency, a state of preventive defence, a state of terrorist threat, an unexpected attack and a state of danger;

c) shall, within the framework of this Act, perform tasks specified by the Government, the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities or the Minister responsible for national defence;

d)

e) shall provide for specialised trainings for the professional personnel and the law enforcement administration and national defence employees.

Direction and control of national security services

Section 10 (1) The Government shall direct

a) the Information Office through the Minister responsible for the direction of civilian intelligence activities,

b) the Constitution Protection Office, the Special Service for National Security and the Counter-Terrorism Information and Criminal Analysis Centre through the Minister responsible for the direction of civilian national security services,

c) the Military National Security Service through the Minister responsible for national defence

[Ministers under points *a)* to *c)* hereinafter jointly "Minister"].

(2) The Minister responsible for the direction of civilian national security services shall have the power to exercise direction regarding the processing of data of public interest and data accessible on public interest grounds processed by the Counter-Terrorism Information and Criminal Analysis Centre.

(3)

Section 11 (1) The Minister

a) shall prepare, or participate in the preparation of, drafts of laws and other governmental decisions relating to the operation, functions and powers of national security services;

b) shall ensure the performance of national security tasks related to the enforcement and protection of the interests of Hungary;

c) shall regulate the activities and operation of national security services by way of decrees and normative instructions;

d) shall maintain relations to facilitate international cooperation between national security services.

(2) Within his power to exercise direction, the Minister

a) shall allocate tasks and give instructions to national security services for the performance of tasks set out by Acts, government decrees or other governmental decisions;

b) shall provide the directors-general with timely tasks for the services every six months in writing; shall give written instructions to fulfil information needs received from members of the Government;

c) shall approve the organisational and operational regulations and the organisational chart of national security services upon a submission by the directors-general;

d) shall make proposals on the budget of national security services;

e) regarding the budget management of national security services, shall perform the duties and exercise the rights, prescribed by law, of a head of an organ responsible for a budget heading, or a head of an organ responsible for the supervision of a budgetary organ, that are related to planning, modifying appropriations, reporting, providing information, finances or supervision;

f) shall supervise the expediency and efficiency of the budget management of national security services;

g) shall supervise the lawful and proper operation of national security services and the performance of their tasks;

h) shall, upon a submission by the directors-general, approve the internal rules on the procedure of, and on providing permission for, secret information gathering;

i) shall, upon a submission by the directors-general, approve proposals regarding the international relations of national security services;

j) shall make proposals on the appointment and dismissal of directors-general to the Prime Minister;

k) shall exercise employer's rights, other than the rights of appointment and dismissal, over directors-general; shall appoint, dismiss, and exercise employer's rights over, their deputies;

l) shall make proposals on the appointment of generals to the President of the Republic;

m) shall appoint colonels upon proposals by the directors-general;

n) shall approve the appointment of persons proposed for positions with the rank of general and the dismissal of persons in those positions;

o) shall provide for internal security and crime prevention checks with respect to directors-general and their deputies;

p) shall exercise special rights granted by an Act, government decree or government decision.

(3) An instruction by a Minister issued within his power to exercise direction shall not remove a case from, or prevent the exercise of, the competence of directors-general.

(4) The Minister may issue individual instructions to national security services through the directors-general, but he may not instruct national security services proceeding with official authority as to the content of their decisions.

(5) The Minister shall investigate complaints concerning the activities of national security services and shall, within 30 days, inform the complainant about the result of the investigation and about measures taken. This time limit may be extended once by 30 days.

(6) In respect of the Constitution Protection Office and the Special Service for National Security, the Minister responsible for the direction of civilian national security services, while in respect of the Information Office, the Minister responsible for the direction of civilian intelligence activities, shall direct the analysis and evaluation of information from state organs regarding the national security of the country, and the activities supporting the preparation of the relevant governmental decisions. The Minister responsible for the direction of civilian national security services shall, through the Counter-Terrorism Information and Criminal Analysis Centre, direct the analysis and evaluation of information from state organs regarding security and criminal situation, and the activities supporting the preparation of the relevant governmental decisions.

(7) The organ performing internal crime prevention and crime detection tasks, as specified in the Act on the police, shall carry out the internal crime prevention and crime detection checks at the Constitution Protection Office, the Special Service for National Security and the Counter-Terrorism Information and Criminal Analysis Centre.

Section 11/A (1) In respect of the Constitution Protection Office, the Minister responsible for the direction of civilian national security services, in respect of the Information Office, the Minister responsible for the direction of civilian intelligence activities, while in respect of the Military National Security Service, the Minister responsible for national defence shall perform the tasks of national central access points designated under Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

(2) In order to verify the lawfulness of data retrieval and ensure the integrity and security of data, the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities and the Minister responsible for national defence shall keep a data transfer log of access, for consultation purposes, to the visa information system (hereinafter the “Visa Information System”) established by Council Decision 2004/512/EC.

(3) Data included in the data transfer log may be used in accordance with Article 34 (2) of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), and shall be deleted after the period specified therein.

(4) The data transfer log shall contain the following data:

a) the exact purpose of the access for consultation purposes, including the criminal offence under section 45 (2) concerned in the specific case,

b) the reference number of the case concerning which access for consultation purposes is initiated,

c) the date and exact time of access,

d) in case of an urgent procedure, a reference to this fact,

e) data required for the access for consultation purposes that are included in the initiative,

f) the type of data consulted,

g) the identification code provided by the VIS national central authority to persons authorised to conduct search by the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities, or the Minister responsible for national defence, and

h) the identification code provided by the VIS national central authority to persons authorised to initiate access for consultation purposes by the director-general of the Constitution Protection Office, the Information Office or the Military National Security Service.

(5) To ensure the traceability of access for consultation purposes, the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities, and the Minister responsible for national defence shall keep a record of the name and identification code of persons authorised to conduct search and initiate access for consultation purposes during the period of their access authorisation.

Section 12 (1) The head of a national security service shall be the director-general, who is appointed and dismissed by the Prime Minister upon a submission by the Minister.

(2) The submission regarding the director-general of the Special Service for National Security shall be made by the Minister responsible for the direction of civilian national security services in agreement with the Minister responsible for national defence and the Minister responsible for law enforcement.

Section 12/A

Section 13 (1) The directors-general shall be individually responsible for the direction of national security services within the framework provided in this Act, by laws and by public law regulatory instruments.

(2) The commander of the Hungarian Defence Forces may request the transmission of information required for the performance of his tasks under the Act on national defence directly from the director-general of the Military National Security Service, even if no superior-subordinate relationship exists between them, who shall comply with such request without delay. The rules on professional communication and information provision shall be determined by the Minister responsible for national defence.

(3) The director-general

a) shall be responsible for the lawful, proper and professional operation of the national security service and for the performance of the tasks of the national security service;

b) may give instructions to the national security service under his control;

c) shall be responsible for the autonomous budgetary management, and the performance of accounting and reporting obligations, of the national security service;

d) shall, with the exception of the director-general of the Counter-Terrorism Information and Criminal Analysis Centre, determine the internal rules on the procedure of, and on providing permission for, secret information gathering, with approval of the Minister;

e) shall determine the internal procedural rules of data processing;

f) shall provide for the preparation of organisational and operational regulations and of other internal regulations, and ensure the establishment and enforcement of their coherence;

g) shall make proposals to the Minister on the appointment or dismissal of deputy directors-general and on the appointment of generals and colonels;

h) shall submit for approval the appointment and dismissal of persons in positions with the rank of general;

i) shall exercise employer's rights over the personnel of the national security service, with the exceptions specified by law;

j) shall, through the Minister, report to the Government about the activities of the national security service as necessary, but at least once a year.

(4) For the purposes of paragraph (1), public law regulatory instruments shall be construed to also mean other legal instruments of state administration.

Parliamentary monitoring of national security services

Section 14 (1) The National Assembly shall carry out the parliamentary monitoring of national security services with the assistance of the Committee on National Security (hereinafter the "Committee"). The chair of the Committee shall always be an opposition Member of the National Assembly.

(2) The Minister shall inform the Committee of the general activities of national security services regularly, but at least twice a year.

(3) The Government shall inform the Committee about its decisions related to national security services through the Minister.

(4) During the exercise of parliamentary monitoring, the Committee

a) may request information about the national security situation of the country and the operation and activities of national security services from the Minister and, by notifying the Minister simultaneously, from the directors-general of national security services;

b) may request information about the permission procedures under sections 56 and 59 from the Minister responsible for justice, the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities, the Minister responsible for national defence and the directors-general;

c) may investigate complaints against the unlawful activities of national security services if the complainant does not accept the result of the investigation under section 11 (5) and the gravity of the complaint necessitates investigation according to the votes of at least one third of the members of the Committee; the Committee shall inform the people concerned of its findings;

d) if it assumes that an activity of a national security service is illegal or improper, may invite the Minister to conduct an investigation, who shall inform the Committee of the result of this investigation;

e) if it holds that operation by a national security service is against the law, or if in the course of a procedure set out in points *c)* and *d)* or section 27 (4) it finds it reasonable, may carry out a fact-finding investigation, as part of which it may inspect documents relevant to the case concerned that are included in a register of the national security services, and may hear the staff members of national security services;

f) if it identifies, in any way, an illegal or improper activity of a national security service, may invite the Minister to take the necessary measures, and may initiate the examination of responsibility; the Minister shall inform the Committee of the result of this examination;

g) shall give its opinion on the detailed draft of the budget of national security services, on the budget lines related to secret information gathering of other organs authorised to carry out such activity, and on the detailed draft of the report on the implementation of the annual Act on the budget; and shall make proposals to the National Assembly regarding the adoption of legislative proposals in the course of their discussion;

h) shall hear candidates for the office of director-general prior to their appointment, and shall take a position on their eligibility;

i) shall decide on complaints against the findings of a security expert opinion and against a ministerial decision related to the rejection of ordering a review procedure;

j) shall take a position on information provided by the Commissioner for Fundamental Rights about a review procedure by a national security service.

(5) If it is necessary for exercising its monitoring powers, the Committee may ask a member of the personnel of a national security service to perform expert assistance, simultaneously notifying the competent director-general.

Section 14/A (1) If the Committee carries out a fact-finding investigation under section 14 (4) *e)*, the Committee may oblige a person, organ or organisation possessing documents, data or other information related to the fact-finding investigation to assist in such fact-finding investigation (hereinafter "person obliged to render assistance").

(2) The person obliged to render assistance shall be subject to

a) an obligation to provide data,

b) an obligation to appear, and

c) an obligation to make statements.

(3) With the exception under section 16 (1), it shall not form an obstacle to the performance of the obligations to provide data and to make statements if their subject matter is classified information or other information containing classified data. The Committee shall process such data or information confidentially and shall discuss it in a sitting *in camera*.

(4) The Committee shall adopt its decision on an obligation to assist concerning a member of the Government who directs, or previously directed, a national security service, or a senior political executive, permanent state secretary or deputy state secretary proceeding in these matters with delegated powers, or a person who belongs, or previously belonged, to the personnel of a national security service, with the votes of more than half of the Committee members present, whereas concerning other persons, with a vote of more than two thirds of the Committee members present.

Section 14/B (1) Based on a decision by the Committee, the person obliged to render assistance shall be summoned by the chair of the Committee, by setting a time limit for the performance, in a sitting of the Committee, of his obligation to appear, to provide data and to make statements.

(2) The Committee shall serve the summons by mail. To the service, the provisions of the Act on the Code of Civil Procedure shall apply.

(3) Soldiers [section 127 (1) of the Criminal Code] shall be summoned through their military superior.

(4) The summons shall be served in a way that ensures its receipt by the person summoned at least eight days before the hearing.

(5) The chair of the Committee shall indicate in the summons the case, and the capacity, in which the person summoned is to be heard. The person summoned shall be advised of the consequences of failure to appear, provide data or make a statement.

(6) Upon a decision by the Committee, the chair of the Committee shall, by setting a due date, request a person obliged to render assistance to perform in writing his obligation to provide data or to make a statement. Paragraphs (2) to (5) shall apply accordingly to a request to the person obliged to render assistance.

Section 15 (1) The Committee shall receive the general evaluation reports prepared by national security services, which are significant for national security, and the reports prepared for the Government.

(2) With the exception of those related to individual cases, the Committee shall be entitled to inspect information reports by national security services.

(3) If an information gathering activity is commenced, or pursued, by a national security service regarding a Member of the National Assembly, a national minority advocate, or a relative thereof living in the same household, the Minister shall inform the Committee of this fact without delay. The Member of the National Assembly affected by the case shall not receive information about this activity.

Section 16 (1) In the course of the parliamentary monitoring performed by the Committee, the obligation of the Minister or the national security services to provide information shall not cover, with the exception set out in paragraph (2), the provision of information the transmission of which would threaten particularly significant national security interests concerning the protection of the method or the source (the identity of a cooperating person), in a specific case.

(2) In the course of an investigation concerning the unlawful activities by national security services, and with a two-thirds majority consent, the Committee may oblige the Minister and the director-general to provide data regarding a method used in Hungary for secret information gathering, having knowledge of which is essential for the assessment of unlawfulness. Data consulted in this way shall be used only in the proceeding of the Committee.

Section 17 (1) The Committee on National Defence of the National Assembly (hereinafter the "National Defence Committee") shall continuously monitor the performance of the tasks of the Military National Security Service; and within this framework,

a) the Minister shall inform the National Defence Committee about the general activities of national security services at least once a year;

b) the Minister shall inform the National Defence Committee of government decisions concerning the Military National Security Service;

c) the National Defence Committee shall hear the candidates for the office of director-general of the Military National Security Service prior to their appointment, and shall take a position on their eligibility.

(2) Members of the National Defence Committee shall be elected only from among the Members of the National Assembly who have been subjected to national security vetting in accordance with the procedure set out in section 19.

(3) Members of the National Defence Committee shall be under national security protection for the entire duration of their mandate.

Section 18 (1) The Committee, when exercising its monitoring powers, and the National Defence Committee, when exercising its powers specified in section 17, shall sit *in camera*.

(2) Members of the Committee, and of the National Defence Committee, shall be subject to an obligation of confidentiality relating to information containing classified data received in their capacity as such, which shall survive the termination of the Committee membership.

(3) Judicial or other proceedings specified by law shall not be affected by the parliamentary monitoring proceedings of the Committee under this Act.

(4) The Committee shall formulate its responses to complaints and notices regarding the lawful operation of a national security service in a way that allows for no conclusions to be drawn regarding the secret information gathering activities of national security services.

Section 19 (1) Members of the Committee shall be elected only from among the Members of the National Assembly who have been subjected to national security vetting as set out in this Act.

(2) The Speaker of the National Assembly shall initiate the national security vetting of Members of the National Assembly nominated to the Committee by the leader of a parliamentary group.

(3)

(4) Regarding Members of the National Assembly nominated to the Committee, the Constitution Protection Office shall, in accordance with section 68 (5), carry out national security vetting.

(5) If a risk factor occurs, the director-general of the Constitution Protection Office shall inform accordingly the Member of the National Assembly concerned and the Minister responsible for the direction of civilian national security services.

(6) After the completion of the national security vetting, the leader of the parliamentary group shall prepare a recommendation with a number of candidates equal to the number of members the parliamentary group is entitled to recommend.

(7) If a risk factor exists with respect to a Member of the National Assembly specified in the recommendation, of which the Member of the National Assembly concerned and the Minister responsible for the direction of civilian national security services was informed, the Minister responsible for the direction of civilian national security services shall inform of the risk factor the Speaker of the National Assembly and the leader of the parliamentary group concerned.

(8) If the leader of the parliamentary group concerned maintains a nomination to the Committee already formed even after having been informed of a risk factor, the Speaker of the National Assembly shall, after obtaining the opinion of the chair of the Committee and the leader of the parliamentary group concerned, decide on the further validity of the nomination.

(9) If the Committee has not yet been formed and the leader of the parliamentary group concerned maintains a nomination in spite of having been informed under paragraph (7), the Member of the National Assembly nominated in this way shall not be elected as the member of the Committee before the chairs of both the Committee and the National Defence Committee are elected. After the chairs of both the Committee and the National Defence Committee are elected, within 8 days of the election of the chair elected later, a decision shall be taken in accordance with paragraph (8) on the validity of the nomination.

(10) If a Member of the National Assembly nominated for chair of the Committee is affected by a risk factor, the Speaker of the National Assembly shall decide on the validity of the nomination.

Section 19/A (1) When investigating a complaint specified in section 14 (4) *i)*, the Committee may inspect the documents of a national security vetting, request information from the Minister and the director-general of the national security service providing a security expert opinion, and hear the complainant.

(2) Based on the investigation, the Committee shall either

a) dismiss the complaint, if unfounded, or

b) uphold the complaint and

ba) oblige the national security service performing national security vetting to conduct a new procedure, in addition to setting aside the decision on identifying a national security risk, or

bb) oblige the director-general of the national security service to order a review procedure, in addition to setting aside the decision on refusing to order a review procedure.

(3) The Committee shall inform the Minister responsible for the direction of the national security service, the complainant and the person entitled to initiate national security vetting of its decision under paragraph (2).

(4) The Committee shall examine the content of information specified in section 14 (4) *j)*, and in the course of doing so, it may request information in writing, or at a personal hearing, from the Commissioner for Fundamental Rights, the Minister responsible for the direction of the national security service and the director-general of the national security service, and may hear the person subjected to the review procedure.

(5) The Committee shall inform the Commissioner for Fundamental Rights, the Minister responsible for direction, the director-general of the national security service and the person initiating the procedure of the Commissioner for Fundamental Rights about its position on the provision of information specified in section 14 (4) *j)*.

Special rules on members of the Committee on Foreign Affairs of the National Assembly

Section 19/B Members of the Committee on Foreign Affairs shall be elected only from among the Members of the National Assembly who have been subjected to national security vetting in accordance with the procedure set out in section 19.

Personnel of national security services

Section 20 (1) The personnel of national security services shall consist of persons in professional service relationship and of law enforcement administration employees and workers, while that of the Military National Security Service shall consist of persons in professional service relationship and of national defence employees and workers.

(1a) Persons in professional service relationship at cooperating organs may be deployed, law enforcement administration employees may be seconded, and employees of the National Tax and Customs Administration may be either deployed or seconded to the Counter-Terrorism Information and Criminal Analysis Centre.

(1b) The Counter-Terrorism Information and Criminal Analysis Centre may be designated as the place of service for persons in a professional service relationship with an organ performing law enforcement duties as specified in the Act on the service relationship of the professional personnel of organs performing law enforcement duties, and for members of the personnel who are deployed to the Military National Security Service in accordance with the Act on the legal status of soldiers.

(2) In addition to those specified in paragraph (1), the personnel of the Military National Security Service shall consist of volunteer reserve soldiers. The professional and volunteer reserve soldiers of the Military National Security Service shall be part of the personnel of the Hungarian Defence Forces. Their service relationship shall be governed by laws pertaining to the service relationship of professional and volunteer reserve soldiers.

(3) The Minister shall be authorised to deploy, for the performance of work, a member of the professional personnel of a national security service to the organisation assisting in the performance of tasks related to direction.

Section 21 (1) The service relationship of the professional personnel of national security services shall be a special service relationship established for an indefinite period, in which service is performed in a chain of command and under highly dangerous circumstances.

(2) Professional service relationship may be established with Hungarian citizens with full capacity to act, who have permanent domicile in Hungary and no criminal record, fulfil the educational and vocational, health, psychological and physical fitness requirements for the service position, and any additional requirements determined by the Minister, and who consent to a security check for the purpose of establishing and maintaining the service relationship, provided that no risk factors were found by the check.

(3) Fitness for service may be tested both at the time of the establishment of a service relationship and during its period.

Section 22 (1) Members of the professional personnel of national security services

a)

b) shall exercise their citizens' rights subject to restrictions set out in this Act and in a separate Act on the service relationship concerned;

c)

d) shall notify the director-general in advance of their intention to join a non-governmental organisation; the director-general may prohibit membership in such an organisation if it is in conflict with the profession or service position concerned, or it interferes with, or threatens, the interests of the service (incompatibility);

e) shall not perform activities that are unworthy of the professional service relationship or that would endanger the impartial performance of service tasks free from influence;

f) may establish, with prior permission by the director-general, other legal relationships involving the performance of work; the permission shall be refused in the cases specified in point *e)*, and also if the establishment of the legal relationship is in conflict with the profession or the service position concerned, or if it may allow for the abuse of information obtained in connection with the service relationship, or if it interferes with, or threatens, the interests of the service.

(2) Members of the professional personnel of national security services

a) shall take an oath,

b) shall perform their tasks related to their service position, in accordance with the provisions of Acts,

c) shall obey instructions by their superior, taking into account section 27,

d) shall enforce the national security interests of Hungary by every lawful means and protect them even at the cost of their lives.

Section 23 (1) Law enforcement administration and national defence employees shall perform tasks at national security services which do not require the establishment of a professional service relationship demanding special requirements.

(2) National security services may establish law enforcement administration service, and national defence employment, relationships only with persons meeting the employment requirements set out by the Acts on the service relationship of law enforcement administration employees and on the legal status of national defence employees, provided that no national security risk has been identified by the national security vetting performed in connection with the establishment and maintenance of the legal relationship.

(3) The professional service position may be reclassified as a law enforcement administration, or a national defence, employment position, while a law enforcement administration, or a national defence, employment position may be reclassified as a professional service position. To reclassified legal relationships, the provisions laid down by a separate Act shall apply.

Section 24 The personnel of national security services shall keep confidential any classified data acquired by them relating to national security services and their activities, this obligation shall also include the retention and protection of classified data. The Minister and the directors-general of national security services may grant exemption from this confidentiality obligation. The obligation of confidentiality of the personnel of national security services shall survive the termination of their employment.

Section 25

Operating principles of national security services

Section 26 The detailed rules of the internal organisation and operation of national security services and the rules for giving instructions shall be established in a way that allows, at all times, for the identification of the person individually responsible.

Section 27 (1) When performing his tasks, a member of the professional personnel of a national security service shall execute the instructions of his service superior, unless it is obvious that he would commit a criminal offence by doing so.

(2) If a member of the professional personnel of a national security service refuses, under paragraph (1), to execute an instruction received, he shall report this fact to the director-general. The director-general shall forward this report to the Minister and the Committee without delay.

(3) If a member of the professional personnel of a national security service receives an instruction for an unlawful activity, he shall notify the person giving the instruction of this fact, but with the exception specified in paragraph (1), the execution of such instruction may not be refused.

(4) If a member of a national security service detects the unlawful operation of a service, he may report his observation in writing to the Minister. The Minister shall be obliged to investigate such report, and to inform the Committee and the reporting person about ordering, and the results of, the investigation.

Section 28 (1) National security services shall cooperate with each other for the performance of their tasks.

(2) State organs, local governments and national security services shall mutually help the work of each other. The detailed rules of cooperation shall be set out in separate agreements within the framework of provisions of an Act.

(3) National security services may cooperate with natural persons, legal persons or organisations without legal personality in the performance of their tasks. The detailed rules of cooperation may be set out by separate agreements within the framework of provisions of an Act.

(4) National security services may cooperate with foreign secret services under international agreements and commitments. In addition to the foregoing, the Counter-Terrorism Information and Criminal Analysis Centre may, with approval by the Minister responsible for the direction of civilian national security services, maintain direct relations with international organisations or foreign police, administrative, law enforcement and national security organs and organs established by foreign States for the furtherance of such goals.

(5) In order to enforce safety requirements and within the framework of provisions of an Act, national security services shall establish, in separate agreements concluded with the competent organisations, the procedural rules related to social security, to healthcare, to tax settlement, to budget, financial and statistical data provision, to checks of archives for the protection of documents of lasting value, and to the use of currency as a part of special operating costs.

Section 29 (1) Within the area of their responsibilities and the framework of this Act, members of the Government may request the Minister in writing to specify information needs for national security services. The request shall be justified and shall indicate that the information cannot be obtained from another source.

(2) As set out by the Government, state organs shall provide data in the domains of information necessary for the activity specified in section 11 (6), free of charge.

Section 30 (1) In order to fulfil the tasks under this Act, if it is initiated by directors-general of national security services, state organs of particular importance for national security, economic operators under long-term state ownership, and factories and institutions operating central energy supply and communications systems, producing and using internationally controlled products and technologies, or carrying out defence industry research shall establish professional, public, governmental or tax and customs authority service relationship, or public employment, law enforcement administration service, or national defence employment relationship or employment relationship (hereinafter jointly “employment relationship”) with the personnel of a national security service otherwise meeting the employment requirements.

(2) For the performance of tasks under this Act, national security services may initiate the establishment of employment relationship for the period specified in a separate agreement with organisations not falling under the scope of paragraph (1).

(3) National security services shall not initiate the establishment of an employment relationship with a court, the prosecution service, the Constitutional Court, the State Audit Office, the National Authority for Data Protection and Freedom of Information, the Office of the Commissioner for Fundamental Rights, the Office of the President of the Republic and the Office of the National Assembly.

(4) Within the framework laid down by the legislation in force, the special rules pertaining to the national security nature of the employment shall be set out in a separate agreement between the national security services and the organisation concerned.

Special provisions relating to the operation of the Counter-Terrorism Information and Criminal Analysis Centre

Section 30/A Cooperating organs shall be the following:

a) an organ established to carry out general policing tasks as specified in the Act on the police,

b) an organ with internal crime prevention and crime detection tasks as specified in the Act on the police,

c) a counter-terrorism organ as specified in the Act on the police,

d) the National Tax and Customs Administration,

e) civilian national security services,

f) the Military National Security Service,

g) the immigration authority,

h) the asylum authority,

i) an organ proceeding in citizenship matters,

j) the central organ of the prison service,

k) the organ maintaining criminal records,

l) the central organ of the professional disaster management organ,

m) the central organ keeping the register of the personal data and address of citizens.

Measures applicable by national security services

Section 31 (1) National security services shall not conduct investigations or preparatory proceedings.

(2) Members of the professional personnel of national security services may apply the measures defined in sections 32 to 36 to prevent, and to apprehend the perpetrator of, criminal offences falling within the functions of national security services.

(3) During the performance of their tasks, national security services may restrict, in accordance with this Act, the right to personal freedom, privacy of home, personal secrets, confidentiality of correspondence, protection of personal data, access to data of public interest and protection of possession.

(4) A measure shall not cause harm which is obviously disproportionate to the lawful objective of the measure.

(5) When using any coercive means during the application of measures, injuries shall preferably be avoided.

(6) From among multiple possible and suitable measures and coercive means, that one shall be chosen that ensures effectiveness while causing the least possible restriction, injury or damage to the person affected.

Section 32 Members of the professional personnel of national security services may apprehend and bring before an authority by force the perpetrator of a criminal offence falling within the function of national security services, if caught in the act, and may, for this purpose, use coercion (physical force) to stop an act or to overcome resistance. After apprehension, the perpetrator shall immediately be brought before an authority by force.

Section 33 In a case under section 32, a member of the professional personnel of national security services may use handcuffs

a) to prevent the infliction of self-harm;

b) to prevent attacks;

c) to prevent an escape;

d) to overcome resistance

by the persons whose personal liberty is, or is intended to be, restricted.

Section 34 Members of the professional personnel of national security services shall have the right to carry service firearms. The Minister shall determine the detailed rules related to carrying, using and storing service weapons.

Section 35 (1) Members of the professional personnel of national security services shall be entitled to use firearms in accordance with this Act. Firearms may be used based on individual decision or, in exceptional cases, on command.

(2) Only a deliberate shot at a person shall constitute use of a firearm.

Section 36 (1) With the exception of cases of justifiable defence and necessity, members of the professional personnel of national security services may use firearms

a) to avert attacks on life, or seriously endangering physical integrity, or the direct threat thereof;

b) to prevent or interrupt the commission of the criminal offence of genocide (section 142 of the Criminal Code), changing the constitutional order by force (section 254 of the Criminal Code), destruction (section 257 of the Criminal Code), espionage (section 261 of the Criminal Code), terrorist act (sections 314 to 316/A of the Criminal Code), unlawful seizure of a vehicle (section 320 of the Criminal Code) and causing public danger (section 322 of the Criminal Code);

c) in a case of unauthorised acquisition, by violence against a person, of data classified as "Szigorúan titkos!" ("top secret") related to a national security service, or an attempt thereof;

d) to ward off attacks against, or directly threatening, the facilities of a national security service.

(2) Use of firearms shall be preceded by

a) an instruction to stop the unlawful activity;

b) the use of other coercive means;

c) a warning that a firearm is about to be used;

d) a warning shot.

(3) Measures preceding the use of firearms may be omitted, in whole or in part, if, with regard to all circumstances of the situation, there is no time for precautionary measures, and any delay directly endangers the life or physical integrity of the member of the professional personnel or another person.

(4) When using a firearm, taking someone's life shall be avoided.

(5) The use of a firearm and the firing of a warning shot shall be reported to the service superior, regardless of the consequences, immediately after taking the measure.

(6) With the exception of a case of justifiable defence or necessity, firearms shall not be used against visibly pregnant women and children.

Section 37 (1) Against measures specified in sections 32 to 36 taken by a member of the professional personnel of national security services, a person concerned or, if he is prevented from doing so, his relative, may submit a complaint.

(2) The complaint shall be submitted to the director-general of the national security service within 8 days of the person concerned becoming aware of the measure. After 5 years from the contested measure, no complaint shall be submitted.

(3) The general-director shall decide on a complaint within 8 days of receipt.

(4) Within 8 days from its communication, the complainant may submit an appeal against a decision to the Minister. The Minister shall uphold, amend or annul the first instance decision within 8 days from receipt.

(5) An application for excuse may be submitted within 30 days following a missed due date.

(6) Launching an administrative court action shall be conditional upon exhausting the option of filing a complaint. This action shall fall within the exclusive territorial jurisdiction of the Budapest-Capital Regional Court. The court shall not amend the decision of the Minister.

Data processing by national security services

Section 38 For the performance of their tasks specified in this Act, national security services may process

a) personal data, sensitive data and criminal personal data, as well as

b) data of public interest and data accessible on public interest grounds

(those specified in points *a)* to *b)* hereinafter jointly "data").

Section 39 (1) National security services may acquire data

a) by way of voluntary or, if this Act so provides, mandatory, provision of data by a person concerned;

b) from an open source;

c) by way of provision of data by an organ processing data;

d) through direct electronic data link, in cases specified in this Act;

e) by way of secret information gathering, with the exception specified in paragraph (1a)

(1a) The Counter-Terrorism Information and Criminal Analysis Centre shall not carry out secret information gathering.

(2) In the course of data processing, national security services shall use means which are strictly necessary for the specific purpose, but restrict the personality rights of the person concerned to the least extent possible.

(3) Persons subject to national security vetting shall provide the data necessary for national security vetting to the national security service carrying out the national security vetting.

Section 40 (1) Unless otherwise provided by an Act, for the performance of their tasks, national security services may request, properly indicating the purpose of request, data from any data processing system, and may inspect any documents serving as a basis for the records. Based on a data request, state organs, companies under majority state ownership and financial institutions specified in the Act on credit institutions and financial undertakings shall transfer data in an electronic form, through electronic data link, by using an interface built and operated free of charge by the data controller in compliance with the technical specifications set out by the national security service concerned, and such data transfer shall also be performed regarding incomplete and fragmentary data.

(1a) Transmitting organs shall keep separate records of data transfers under paragraph (1) which do not allow for subsequent modifications registering the fact and the date of data transfers and the unique identifiers generated by data recipients at the date of a data request, while recipient organs shall keep separate logs of data transfers under paragraph (1) which do not allow for subsequent modifications registering the fact and the date of data transfers, the unique identifiers and the purpose of data requests. Data regarding certain data transfers may be deleted from the logs after five years from the data transfer concerned.

(1b) Data controllers shall establish, for the national security service concerned, the technical system meeting the requirements set out in paragraph (1) within six months of obtaining written information about the technical specifications.

(2) National security services may request and use data in records kept by state organs, local governments, financial institutions, insurance institutions and telecommunications service providers free of charge. Other data controller organs may claim costs related to data requests by national security services subsequently.

(3) When requesting data from the central organ keeping the register of the personal data and address of citizens, during communication with the person concerned and other data controllers, and in their records, national security services may use, for the performance of their tasks under this Act and as provided by law, personal identifiers, natural identification data, tax identification numbers and other identifiers.

(4) For the performance of their tasks, national security services are entitled to receive image, sound or audio-visual recordings recorded by a state organ or local government operating, in public spaces, devices suitable for making image, sound or audio-visual recordings.

Section 41 (1) For the performance of their tasks, national security services may order the placement of watch-listing annotations,

a) in the records of state or local government organs keeping records on, or processing, the personal data, and data relating to the address, of citizens,

b) in the records of the ministry led by the Minister responsible for keeping the register of the personal data and address of citizens,

c) in the records of the organ established to carry out general policing tasks,

d) in the real estate register,

e) in the company register,

f) in record systems for border traffic control,

g) in the records of every organ authorised to record, for any purpose, motor vehicles and their registration marks,

h) in the records of organs processing health data and other related data,

i) in the records of organs processing data constituting bank, payment, securities, fund or insurance secret, or other trade secret, and providing services available to everybody and accessible by anyone,

j) in the records of state and local government tax authorities,

k) in the records of postal service providers,

l) in the systems of electronic communications service providers,

in a documented manner allowing for their preservation and indicating the purpose, the date and the time limit or the duration of the measure, and they may operate watch-listing systems regarding such annotations.

(2) In a watch-listing annotation, national security services may ask for a change in data, or in case of a request regarding the person concerned, the provision of notification; and with respect to cross-border traffic, they may also ask for the interception of the person concerned in writing. The organ concerned shall take the measure specified in a request by the national security services.

(3) National security services shall provide for the removal of a watch-listing annotation without delay, if the circumstance serving as ground for it ceases to exist.

(4) Measures for placement of watch-listing annotations and the operation of the watch-listing system shall be carried out in an electronic form, if the records allow for it, and with the processing of data being properly documented; and if possible, through electronic data link, by using an interface built and operated by the organ providing the data in accordance with paragraphs (6) and (7) in compliance with the technical specifications set out by the national security service operating the watch-listing system.

(5) The organ providing data shall establish, for the national security services operating the watch-listing system, the technical system meeting the requirements set out in paragraph (4) within six months of obtaining written information about the technical specifications.

(6) The watch-listing system specified in paragraph (1) shall be established and operated by state organs keeping the records under paragraph (1) and by companies under majority state ownership, from their own budget.

(7) Unless otherwise provided by an Act, organs and companies other than those specified in paragraph (6) shall establish and operate the watch-listing system under paragraph (1) from the budget of the national security service operating the watch-listing system.

Section 41/A (1) Civilian national security services may initiate, at the police, the placement of alerts for discreet checks in the Schengen Information System, if the data acquired indicate that it is necessary for the enforcement of the national security interests of Hungary.

(2) In the event specified in paragraph (1), civilian national security services may initiate the placement of alerts for discreet checks only after the receipt of information under Article 36 (3) of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

Section 41/B In addition to the provisions of sections 41 to 41/A, the Counter-Terrorism Information and Criminal Analysis Centre may, in cases falling within its competence, order the placement of watch-listing annotations in the data processing systems of cooperating organs, but only for the purpose of requesting notification, with indicating its purpose, regarding the generation of, and change in, individually specified data.

Section 42 (1)

(2) The data controller organ which provided data to national security services from the records kept by it, ensured access to data or placed a watch-listing annotation in its records upon a request by the national security services shall not inform the persons concerned or other persons or organisations of this fact, about the content thereof, or about any measures taken.

(3) The head of a data controller organ or institution not vested with official powers, may submit a complaint without suspensive effect to the Minister, against ordering access to, or provision of, data.

Section 43 National security services may use the data acquired only for the purpose serving as legal basis for ordering data collection, unless the data

a) indicate that the statutory elements of a criminal offence have been fulfilled, and their transmission is permitted by an Act, or

b) establish an obligation to provide information to another national security service, if the data recipient itself is also entitled to receive the data.

Section 44 (1) Under this Act, national security services may request data from, and shall be obliged to provide data to, each other for the performance of their tasks.

(2) The Police, the National Tax and Customs Administration, the courts, the prosecution service and the prison service may request, indicating the specific purpose, data from national security services for the performance of their tasks and in the scope set out in the relevant Acts.

(2a) National security services shall not be obliged to initiate criminal proceedings and to transmit data, if doing so would jeopardise the performance of their tasks under this Act.

(3) Data provision by national security services shall not result in the disclosure of a person cooperating with national security services (data source). For the protection of the method and the source of secret information gathering, directors-general of national security services may impose restrictions on the use of data transmitted.

(4) Organs requesting data shall be responsible that the received data is processed in accordance with this Act and with the laws on data processing; they shall be obliged to keep a record of data received and their use, and shall, upon request, inform the national security service about it.

Section 45 (1) Under international commitments and within the framework of laws on the protection of personal data, national security services may transfer personal data to foreign data controllers.

(2) The Constitution Protection Office, the Information Office and the Military National Security Service may initiate access for consultation of the Visa Information System in specific individual cases in order to prevent and detect, and to acquire information connected to, criminal offences concerning their competence under this Act, including the task of the Information Office specified in section 4 *c)*. Access for consultation of the Visa Information System (VIS) under Council Decision 2008/633/JHA of 23 June 2008 by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences shall be initiated at the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities, or the Minister responsible for national defence.

(3) Access for consultation under paragraph (2) may be initiated in writing or by electronic means if

a) based on the data available to the initiating party, there is reasonable ground to believe that the prevention or detection of, or the acquisition of information related to, a criminal offence specified in paragraph (2) cannot be effectively ensured without the data available through access for consultation;

b) access for consultation is necessary in a specific procedure aimed at the prevention or detection of, or the acquisition of information related to, a criminal offence falling within the scope of the criminal offences specified in paragraph (2).

(4) An initiative for data provision aimed at access for consultation of the Visa Information System via the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities or the Minister responsible for national defence, shall contain the following data:

a) data verifying that the conditions specified in section (3) *a)* are met,

b) the name of the proceeding authority, the reference number of the specific case, the name of the party with the right of initiative and his identification code provided by the VIS national central authority,

c) the qualification of the criminal offence serving as a ground for the initiative, and

d) the designation of data requested by the initiative and, for each individual piece of data requested, the reasons substantiating that the condition specified in section (3) *a)* is met.

(5) In order to consult the data specified in section (4) *d)*, on the basis of the below-specified data serving for the purpose of search, the scope of data that is accessed for consultation shall be specified, in the initiative, from among the following:

a) family name, family name at birth (former family name); given names; sex; date, place and country of birth,

b) current nationality and nationality at birth,

c) type and number of travel documents, the issuing authority and the date of issue and of expiry,

d) main destination and intended duration of stay,

e) purpose of travel,

f) intended date of arrival and departure,

g) intended border of first entry or transit route,

h) domicile,

i) fingerprints,

j) type of visa and the number of the visa sticker,

k) details of the person issuing an invitation or liable to pay subsistence during the stay.

(6) Before complying with an initiative, the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities or the Minister responsible for national defence, shall examine the fulfilment of the conditions specified in paragraphs (2) to (5) and the justification for the initiative.

(7) In an exceptional case of urgency, the Minister responsible for the direction of civilian national security services, the Minister responsible for the direction of civilian intelligence activities or the Minister responsible for national defence may also grant access for consultation based on an oral initiative by the national security services. In such a case, the fulfilment of the conditions specified in paragraphs (2) to (5) and the justification for the initiative shall be examined, together with the justification for urgency, after complying with the initiative.

(8) If the conditions specified in paragraphs (2) to (5) are not fulfilled, data shall not be received or transferred from the Visa Information System by access based on an initiative. If the designated national central access point under Council Decision 2008/633/JHA complies with the initiative by granting access, and such access results in a hit in the Visa Information System, in addition to the data specified in the initiative, the following data may also be transferred to the initiating national security service:

a) any other data taken from the visa application form,

b) photographs, and

c) any data concerning a visa issued, refused, annulled, revoked or extended previously.

(9) Only persons authorised, based on their tasks, by the director-general of the Constitution Protection Office, the Information Office or the Military National Security Service shall be entitled to initiate access for consultation, provided that the director-general concerned notified the VIS national central authority of this fact. After the notification, the VIS national central authority shall provide the person with the right of initiative with an identification code under section (4) *b)*. The authorisation shall be withdrawn from a person if his task serving as basis for authorisation no longer exists, and the VIS national central authority shall be notified of this fact.

Section 45/A (1) Unless otherwise provided by an international agreement or commitment, at a request by the secret service of another EEA state, national security services shall assist in carrying out repository checks in the course of proceedings subject to the same considerations as national security vetting under this Act (security vetting), and while doing so, they shall be entitled to request data from other state organs processing data, taking into account the aim of the request by the secret service of another EEA state.

(2) National security services shall transmit data generated in the course of their proceedings to the secret service of the EEA state if this data transmission does not interfere with national security interests.

(3) The director-general of a national security service may impose restrictions on the use of data transmitted based on a request.

Section 46 National security services shall keep a log of the transmission of personal data, which shall contain the following:

a) request for data;

b) log identifier of the person requesting data;

c) date of data transmission;

d) the duplicates of documents providing data and of other documents.

Section 47 (1) With the exception provided for in paragraph (3) and for the performance of their specific tasks, national security services may link their data processing systems to the data processing systems of each other or of other state organs processing data, provided that the other data controller also ensures the level of personal data protection prescribed by the Act on the right to informational self-determination and on the freedom of information, and the fulfilment of data security requirements.

(2) The link shall be removed after the performance of the specific national security task, and the data set generated during the period of the systems being linked shall be deleted after the proceeding is completed. Data generated as a result of such linking shall not be deleted if they are necessary for the performance of the tasks of the national security services.

(3) Other national security services may not link the data processing system of the Counter-Terrorism Information and Criminal Analysis Centre to their own data processing systems.

(4) The Counter-Terrorism Information and Criminal Analysis Centre may link its data processing system to the data processing systems of other national security services without the restriction specified in paragraph (2) if the level of personal data protection prescribed by the Act on the right to informational self-determination and on the freedom of information is ensured.

Section 48 (1) If national security interests or the protection of the rights of others so require, the director-general of a national security service may refuse the provision of information, at a request by the person concerned, about data processed by the national security services, or from the data transfer log specified in section 46, the deletion of personal data of the person concerned or a request to consult data of public interest processed by the national security service.

(2) National security services shall keep records of requests by the persons concerned, and shall inform annually the National Authority for Data Protection and Freedom of Information of such requests, the method of their evaluation and the reasons for dismissals.

(3) Regarding classified data of national security services, the director-general of a national security service may, if national security interests so require, restrict the right to consult data provided to the person concerned by the Act on the protection of classified data.

Section 49 (1) Directors-general shall ensure the prevention of unauthorised access to data and of the disclosure, changing, deletion or destruction of such data, and shall provide protection against undue access (data security).

(2) National security services shall regularly verify the accuracy of personal data processed by them. Incorrect data shall be rectified; in the course of data processing, data based on facts shall be distinguished from data based on conclusion, opinion or estimation.

(3) National security services shall process data related to their official functions separately from other data.

Section 50 (1) For the performance of the task defined in this Act, national security services may receive and process, from the records of organs authorised to process data,

a) data of security documents for 10 years from the date of expiry;

b) documents issued in the course of the supervision and direction of encryption-related activities for 10 years from the date of expiry;

c) data generated during the performance of national security vetting and protection tasks for 20 years from the end of a term of the post or the office concerned;

d) personal data gathered while performing a task not specified in points *a)* to *c)* for 70 years from the termination of data gathering;

e) data regarding registration marks of motor vehicles processed in the vehicle register under the Act on the road transport register, and their image data, for 10 years.

(2) Personal data processed by national security services shall be deleted without delay if

a) the time limit specified in paragraph (1) has expired;

b) a court ordered the deletion of the data in the course of a data protection proceeding;

c) the data is processed unlawfully;

d) in the case specified in section 60 (2);

e) the processing of the data is obviously unnecessary.

(3) With the exception of the cases specified in paragraph (2) *b)* to *d)*, the deletion obligation shall not extend to personal data stored on a data-storage medium to be handed over for preservation in an archives under the law on the protection of archival materials.

Section 51 (1) In addition to classified data, data related to

a) facilities and personnel,

b) equipment procurements and other contracts, and

c) security vetting and protection tasks

of national security services may be disclosed only with consent of the Minister or the directors-general.

(2) National security services shall inform annually the National Authority for Data Protection and Freedom of Information of the dismissal, and the reasons for the dismissal, of requests to consult data specified in paragraph (1).

Section 52

Special provisions on data processing by the Counter-Terrorism Information and Criminal Analysis Centre

Section 52/A (1) The Counter-Terrorism Information and Criminal Analysis Centre may acquire data from cooperating organs in accordance with sections 52/B to 52/G only for the performance of the tasks specified in section 8/A (1) to (3).

(2) The Counter-Terrorism Information and Criminal Analysis Centre shall not acquire data generated in connection with the tasks of the police organ with internal crime prevention and crime detection tasks specified in section 7 (1) *b)* of Act XXXIV of 1994 on the Police.

(3) The Counter-Terrorism Information and Criminal Analysis Centre and the Office of the Prosecutor General shall set out in an agreement the scope of data, information and documents that may be transmitted by electronic means and the detailed data provision procedure for the revelation by the Counter-Terrorism Information and Criminal Analysis Centre of any concurrent secret information gathering or concurrent use of covert means, and any concurrent investigation and preparatory proceeding pursuant to the Act on criminal procedure that is carried out by the cooperating organs and the prosecution service and launched after the conclusion of the agreement, and for facilitating such activities.

Section 52/B (1) The Counter-Terrorism Information and Criminal Analysis Centre shall acquire data necessary for exercising the powers and functions of the Counter-Terrorism Information and Criminal Analysis Centre specified in section 8/A (1) to (3) that is processed by cooperating organs

a) through direct electronic data link from data processing systems containing such data, unless otherwise provided in this Act,

b) by any other means ensuring direct and full access to the data processing system containing such data, but primarily by electronic data-storage media specified by the Counter-Terrorism Information and Criminal Analysis Centre.

(2) In cases where it does not jeopardise the effective performance of the tasks, specified in laws, of cooperating organs, the Counter-Terrorism Information and Criminal Analysis Centre may only acquire data regarding the security and criminal situation from the data processing systems of cooperating organs specified in section 30/A *e)* to *f)* through direct electronic data link; in any other case, data shall only be acquired through a individually initiated, unlinked, independent and non-continuous search.

(3) The Counter-Terrorism Information and Criminal Analysis Centre may only acquire, in the way prescribed in paragraph (1) *b)*, the data in the data processing system of cooperating organs specified in section 30/A *g)* to *m)* if the data cannot be acquired in the way prescribed in paragraph (1) *a)*.

(4) The Counter-Terrorism Information and Criminal Analysis Centre may acquire the data in the data processing system of cooperating organs specified in section 30/A *a)* to *e)* also in the way prescribed in paragraph (1) *b)* even if the condition set out in paragraph (3) is not met.

(5) Data in the data processing systems of cooperating organs specified in section 30/A *a)* to *f)* may be acquired only by a member of the professional personnel of the cooperating organ concerned who serves at the Counter-Terrorism Information and Criminal Analysis Centre under section 20 (1a) or (1b).

Section 52/C (1) Cooperating organs shall bear the costs of building and operating a direct electronic data link interface providing access to the data processing system of a cooperating organ and shall provide data access through it for the Counter-Terrorism Information and Criminal Analysis Centre free of charge.

(2) When establishing direct electronic data link, it shall be ensured that

a) it enables access only to data specified in section 52/B (1),

b) it does not result in the disclosure of the identity of persons providing information to the cooperating organ within the framework of secret cooperation,

c) its legality, purpose limitation and the personal liability of persons having access, under section 52/G, to the data can be determined,

d) it does not endanger the effective operation of cooperating organs.

(3) The provisions of paragraph (2) shall apply accordingly to the data link under section 52/B (2).

(4) The Counter-Terrorism Information and Criminal Analysis Centre shall not modify, or enter, data in data processing systems of cooperating organs through direct electronic data link.

(5) The fact of a data provision under section 52/B shall be recorded, in accordance with the Act on the right to informational self-determination and on the freedom of information, both at the cooperating organ and the Counter-Terrorism Information and Criminal Analysis Centre.

(6) In the case of classified data originating from the North Atlantic Treaty Organisation, a body of the Council of the European Union, the European Commission, the European Atomic Energy Community, the European Union Agency for Law Enforcement Cooperation or the European Judicial Cooperation Unit, or a foreign secret service, the head of the cooperating organ shall decide on the transmission of data.

Section 52/D For the purposes of national security, the Counter-Terrorism Information and Criminal Analysis Centre shall also acquire and process data made available to it by foreign bodies under an international treaty promulgated by an Act or under a legally binding act of the European Union within the scope of data, and for the duration, specified therein.

Section 52/E (1) Taking into account section 8/A (3), the Counter-Terrorism Information and Criminal Analysis Centre shall transfer data processed by it to the prosecution office or cooperating organ with related powers that is authorised to process such data, provided that the prosecution office or cooperating organ is entitled to process the data under an Act and processing the data is necessary for exercising its powers and performing its functions.

(2) Having regard to national security and law enforcement interests, the head of a cooperating organ may make subject to his prior consent the use in a criminal proceeding, or the transfer to another specific cooperating organ or other state organ processing data, of data generated by secret information gathering and accessed through electronic data link by the Counter-Terrorism Information and Criminal Analysis Centre, or provided to it by any other means.

(3) The head of the prosecution office having relevant material and territorial competence may make subject to his prior consent the use in a criminal proceeding, or the transfer to a specific cooperating organ or other state organ processing data, of data provided to the Counter-Terrorism Information and Criminal Analysis Centre and generated in the course of secret information gathering.

Section 52/F (1) Data related to governmental information activities, analysis and evaluation activities, and the administration of the Counter-Terrorism Information and Criminal Analysis Centre shall be processed separately.

(2) For the purpose of analysis and evaluation activities and governmental information activities, the Counter-Terrorism Information and Criminal Analysis Centre may, in order to perform a specific task, carry out individual data processing by linking separate data processing systems containing data processed by it to each other or to other data processing systems. New data generated in the course of linking such systems and not used for analysis and evaluation activities or governmental information activities shall be deleted without delay.

(3) If a cooperating organ or the prosecution service deleted, from its own data processing system, the data that was acquired from the cooperating organ or provided by the prosecution service, such data processed by the Counter-Terrorism Information and Criminal Analysis Centre shall also be deleted without delay. The prosecution service and the cooperating organ shall notify the Counter-Terrorism Information and Criminal Analysis Centre of the deletion of the data through direct electronic data link.

Section 52/G Data processing systems containing data processed by the Counter-Terrorism Information and Criminal Analysis Centre may only be inspected, and information about or notification of their data content may only be requested, by members, with access authorisation, of the personnel of the Counter-Terrorism Information and Criminal Analysis Centre, the Minister responsible for the direction of civilian national security services acting within its direction powers, and other organs authorised by a cardinal Act.

Section 52/H (1) In the course of the performance of its task set out in section 8/A (4), the Counter-Terrorism Information and Criminal Analysis Centre shall receive, from the provider of air passenger data, and process passenger data.

(2) The purpose of receiving and processing air passenger data is to facilitate the prevention, detection, investigation and prosecution of the criminal offences specified in Annex 3.

(3) The provider of air passenger data shall transmit air passenger data in an electronic format, and in a manner, specified by the Counter-Terrorism Information and Criminal Analysis Centre.

(4) In the course of performing its task specified in section 8/A (4), the Counter-Terrorism Information and Criminal Analysis Centre

a) shall compare air passenger data provided by the provider of air passenger data with data processed for the purpose of analysis and evaluation activities,

b) shall, within the framework of analysis and evaluation activities, perform risk analysis regarding air passenger data, for the purpose of gathering information indicating criminal offences, activities and endeavours specified in paragraph (2), and

c) shall keep a record on air passenger data received.

(5) In cases set out by an Act, the Counter-Terrorism Information and Criminal Analysis Centre may, for the performance of its task specified in paragraph (4) *b)*, receive personal data from other state organs and records, in order to identify a person concerned.

(6) In carrying out the risk analysis under paragraph (4) *b)*, the Counter-Terrorism Information and Criminal Analysis Centre shall perform an automated risk analysis first. If the automated risk analysis results in a hit, the Counter-Terrorism Information and Criminal Analysis Centre shall individually review the hit by non-automated means involving human assistance.

(7) The Counter-Terrorism Information and Criminal Analysis Centre shall act in accordance with section 8/A (3) *i)* if it discovers information regarding a criminal offence specified in Annex 3 within the framework of its analysis and evaluation activities performed in the course of its passenger information activities.

(8) The Counter-Terrorism Information and Criminal Analysis Centre shall process air passenger data received for five years from its receipt by the Counter-Terrorism Information and Criminal Analysis Centre.

(9) Upon expiry of a period of 6 months after its receipt by the Counter-Terrorism Information and Criminal Analysis Centre, air passenger data provided by the provider of air passenger data shall be depersonalised through masking out the following data elements:

a) name of the passenger, including split or divided passenger name record information under Directive (EU) 2016/681 of the European Parliament and of the Council and the number, and names, of passengers related to a specific passenger name record data,

b) contact details provided by the passenger and, in particular, the address of the domicile, and the place of residence, of the passenger and the persons traveling with him, their phone numbers and email addresses,

c) with the exception of transaction data linked to a credit card or a bank account but not related to the travel transaction, all available payment and billing information, if they contain information that could serve to directly identify the passenger or any other person,

d) frequent flyer data information of the passenger processed by air carriers transporting passengers,

e) general remarks under Directive (EU) 2016/681 of the European Parliament and of the Council if they contain information that could serve to directly identify a passenger,

f) transmitted advance passenger information data under Directive (EU) 2016/681 of the European Parliament and of the Council.

(9a)

(10) In order to carry out its task set out in section (4) *b)*, the Counter-Terrorism Information and Criminal Analysis Centre may receive and process personal data that may be processed under this Act and falls within the scope of data included in the records available through the International Criminal Police Organisation's INTERPOL FIND network database of wanted persons and of stolen and lost travel documents.

(11)

(12)

(13)

Section 52/I (1) For law enforcement purposes laid down in section 52/H (2), based on a legal act of the European Union or a bi- or multilateral international treaty, within the scope of data, for the duration and under the conditions specified therein, the Counter-Terrorism Information and Criminal Analysis Centre may transfer air passenger data processed by it, and the result of their processing, to passenger information units of the Member States of the European Union, to competent authorities of the Member States of the European Union under Directive (EU) 2016/681 of the Parliament and of the Council, and to international organisations and data processing systems established by a legal act of the European Union.

(2) For law enforcement purposes laid down in section 52/H (2), based on a legal act of the European Union or a bi- or multilateral international treaty, within the scope of data, for the duration and under the conditions specified therein, the Counter-Terrorism Information and Criminal Analysis Centre and the competent Hungarian authority under Directive (EU) 2016/681 of the Parliament and of the Council may receive air passenger data, and the result of their processing, from passenger information units of the Member States of the European Union, and from international organisations and data processing systems established by a legal act of the European Union.

(3) The competent Hungarian authority under Directive (EU) 2016/681 of the Parliament and of the Council shall notify the Counter-Terrorism Information and Criminal Analysis Centre if it receives, under paragraph (2), air passenger data, or the result of their processing, from passenger information units of the Member States of the European Union.

(4) From third countries, the Counter-Terrorism Information and Criminal Analysis Centre may receive air passenger data for law enforcement and national security purposes under international treaties, within the scope of data specified therein.

(5) To third countries, the Counter-Terrorism Information and Criminal Analysis Centre shall be allowed to transfer air passenger data processed by it if the conditions specified in Article 13 of Council Framework Decision 2008/977/JHA are met and only for the prevention, detection, investigation or prosecution of criminal offences referred to in Annex 3 and based on an international treaty, within the scope, for the duration and under the conditions specified therein, provided that

a) the task of the receiving authority of a third country is to prevent, investigate or detect criminal offences and to conduct criminal proceedings or to enforce criminal sanctions,

b) the Member State from which the air passenger data originates gives prior consent to the transfer of air passenger data to third countries, with the exception set out in paragraph (7) in case of air passenger data originating from another Member State of the European Union.

(6) If air passenger data requested under paragraph (5) *a)* are depersonalised through masking out data elements, the Counter-Terrorism Information and Criminal Analysis Centre may transmit the complete air passenger data, including data suitable for personal identification, only if the request is well-founded and the purpose of the request is the prevention, detection, investigation or prosecution of criminal offences specified in Annex 3, provided that the prosecution service gave permission to the transmission of air passenger data after the reinstatement of their suitability for personal identification. Section 52/L shall apply accordingly to obtaining permission from the prosecution service.

(7) The prior consent of the other Member State of the European Union shall not be required for the transmission to third countries of air passenger data originating from that Member State if

a) it is essential for averting a specific and actual threat related to a criminal offence referred to in Annex 3 against a Member State or a third country, and

b) the prior consent cannot be obtained in due time.

(8) In an urgent case under paragraph (7), the internal data protection officer of the Counter-Terrorism Information and Criminal Analysis Centre shall be notified.

(9) In case of a request from a third country, the Counter-Terrorism Information and Criminal Analysis Centre may give authorisation to the third country concerned to transmit to another third country data received from the Counter-Terrorism Information and Criminal Analysis Centre under an international treaty, for the purpose of the prevention, detection, investigation or prosecution of serious criminal offences referred to in Annex 3 and specified in an international treaty, if the transmission of such data is strictly necessary for the prevention, detection, investigation or prosecution of these criminal offences.

Section 52/J (1) If in the course of the performance of its passenger information tasks, the Counter-Terrorism Information and Criminal Analysis Centre discovers, within the framework of its analysis and evaluation activities, information regarding a criminal offence specified in Annex 3, and no person affected by the criminal offence specified in Annex 3 can be identified within the framework of the analysis and evaluation activity under section 52/H or the risk assessment activity under section 52/N, the Counter-Terrorism Information and Criminal Analysis Centre may request data for the identification of the persons concerned from the police records containing data received from air carriers transporting passengers and from data processed pursuant to section 91/M (4) of Act XXXIV of 1994 on the Police.

(2) The Counter-Terrorism Information and Criminal Analysis Centre shall delete data received under paragraph (1) within twenty-four hours after the receipt of such data or, if an analysis and evaluation activity under section 52/H is carried out, immediately after the completion of the analysis and evaluation activity under section 52/H or after the data transmission set out in paragraph (3).

(3) In a case under section 52/H (7), the Counter-Terrorism Information and Criminal Analysis Centre shall transmit also the data received under paragraph (1) if it used the data received under paragraph (1) within the framework of its analysis and evaluation activity.

Section 52/K Cooperating organs specified in section 30/A *a)* to *f)*, the prosecution service in the course of a criminal proceeding, and a court in the course of a criminal proceeding under section 52/L (2) shall be entitled to request and receive passenger data, and the results of their processing, from the Counter-Terrorism Information and Criminal Analysis Centre for the purpose of the prevention, detection, investigation or prosecution of criminal offences specified in Annex 3, in order to examine the information further or to take the appropriate measures.

Section 52/L (1) If air passenger data were depersonalised through masking out data elements, the Counter-Terrorism Information and Criminal Analysis Centre may transmit the complete air passenger data, including data suitable for personal identification, upon a reasoned request from

a) organs specified in section 52/K, with the exception of a court proceeding in a criminal proceeding,

b) passenger information units of the Member States of the European Union, or

c) competent authorities of the Member States of the European Union under Directive (EU) 2016/681 of the Parliament and of the Council

only if the purpose of the data request is the prevention, detection, investigation or prosecution of a criminal offence specified in Annex 3, and the prosecution service gave permission to the transmission of air passenger data after the reinstatement of their suitability for personal identification.

(2) Upon a request from a court proceeding in a criminal proceeding, the permission by the prosecution service need not be requested; if the conditions specified in section 52/K are met, the Counter-Terrorism Information and Criminal Analysis Centre shall transmit the complete air passenger data, including data suitable for personal identification.

(3) The organ of the prosecution service designated by the Prosecutor General shall decide on granting the permission.

(4) Upon a request under paragraph (1) and for the purpose of granting permission, the Counter-Terrorism Information and Criminal Analysis Centre shall temporarily reinstate the suitability for personal identification of the requested air passenger data depersonalised through masking out data elements suitable for identification.

(5) A request under paragraph (1) shall be sent to the Counter-Terrorism Information and Criminal Analysis Centre by the organs specified therein. The Counter-Terrorism Information and Criminal Analysis Centre shall send the request to the prosecution service within three working days. Upon the submission by the Counter-Terrorism Information and Criminal Analysis Centre, the prosecution service shall decide on granting permission for data transfer within five working days.

(6) If the procedure for obtaining permission by the prosecution service would cause a delay that would significantly jeopardise the objective pursued by the data transmission, at an expressed and substantiated request by an organ specified in paragraph (1) to this effect, the Counter-Terrorism Information and Criminal Analysis Centre may, before a decision is taken by the prosecution service, transmit the passenger data requested. If the prosecution service does not give subsequent permission to the performance of the request, passenger data transmitted earlier based on the request shall be deleted. If the prosecution service does not give permission to the performance of the request, passenger data shall not be transmitted again at a request from the same organ, for the same purpose and based on the same ground before permission is granted by the prosecution service.

(7) The Counter-Terrorism Information and Criminal Analysis Centre shall keep a log of data transferred under an individual permission under paragraph (1). The log shall contain the following:

a) brief justification for disclosing data the suitability for personal identification of which was reinstated,

b) the date of disclosing data the suitability for personal identification of which was reinstated,

c) the scope of data concerned, and

d) the organ at the request of which data, the suitability for personal identification of which was reinstated, was disclosed.

(8) Data specified in paragraph (7) shall be preserved for the same period as air passenger data the suitability for personal identification of which was reinstated, and shall be deleted at the same time as the air passenger data.

Section 52/M As set out in a law, the Counter-Terrorism Information and Criminal Analysis Centre shall provide, annually, the European Commission with statistical information compiled from air passenger data provided thereto; this information shall not contain personal data.

Section 52N (1) Relating to its tasks set out in section 8/A (4), the Counter-Terrorism Information and Criminal Analysis Centre shall receive and process the data recorded by the boatmaster in command of the ship or the operator of the vessel through the electronic interface to meet the preliminary notification obligation under point 3.1.2, that applies to also inland waterways shipping on the basis of point 4.3, of Annex VI of Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (hereinafter "river passenger data").

(2) River passenger data shall be processed and received to facilitate the prevention, detection, investigation and prosecution of the criminal offences specified in Annex 3.

(3) Section 52/H (6) to (8) and (10) and section 52/L shall apply to river passenger data, with the proviso that air passenger data shall be construed to mean river passenger data.

(4) If, when carrying out its analysis and evaluation activities related to its passenger information tasks, the Counter-Terrorism Information and Criminal Analysis Centre discovers any information related to a criminal offence specified in Annex 3, and no person affected by the criminal offence specified in Annex 3 can be identified as a result of the analysis and evaluation activity under section 52/H the applicability of which is based on paragraph (3), then the Counter-Terrorism Information and Criminal Analysis Centre may, for identifying the affected person, request data from the register containing data received pursuant to section 91/M (4) of Act XXXIV of 1994 on the Police.

(5) The Counter-Terrorism Information and Criminal Analysis Centre shall delete data received in accordance with paragraph (4) within twenty-four hours of receipt or, if an analysis and evaluation activity under section 52/H is carried out, immediately following the completion of the analysis and evaluation activity or the data transmission referred to in paragraph (6).

(6) In a situation under section 52/H (7) the applicability of which is based on paragraph (3), the Counter-Terrorism Information and Criminal Analysis Centre shall transmit also data received pursuant to paragraph (4) if it used the data received pursuant to paragraph (4) for its analysis and evaluation activity.

(7) To prevent, detect, investigate and prosecute a criminal offence listed in Annex 3, a cooperating organ referred to in section 30/A *a)* to *f)* and, in the course of a criminal proceeding, the prosecution service and the court, may request and receive river passenger data, and the result of their processing, from the Counter-Terrorism Information and Criminal Analysis Centre with a view to examining the information further or taking the appropriate measures.

(8) Upon the expiry of a period of 6 months after receipt, the Counter-Terrorism Information and Criminal Analysis Centre shall depersonalise, through masking out the specific data elements, river passenger data received by it.

Section 52/O (1) To enable the verification of the lawfulness of data processing operations by electronic means and to ensure the integrity and security of personal data, the Counter-Terrorism Information and Criminal Analysis Centre shall record in an automated data processing system (hereinafter "log system") information relating to data processing operations concerning river passenger data.

(2) Information describing an event relating to a data processing operation carried out in an information technology application supporting the processing of river passenger data (hereinafter "log entry") shall be collected in the log system.

(3) The log entry shall include the following:

a) scope of personal data affected by the data processing operation,

b) legal basis for, purpose of, and reason for the data processing operation,

c) exact time and date of the data processing operation,

d) name and user identification data of the person carrying out the data processing operation, and data describing his activity,

e) data on the retention period,

f) other descriptive and technical data relating to the data processing operation.

(4) Log entries shall be generated of all operations using personal data at the time of the data processing event. To the log entry, accurate and unalterable time data shall be attached.

(5) Data recorded in the log system shall only be accessed and used for verifying the lawfulness of data processing, enforcing data security requirements, conducting a criminal proceeding and for the purpose of detection, national security protection and counterintelligence, information gathering, and national security and crime prevention vetting as set out in an Act.

(6) Upon request, the Counter-Terrorism Information and Criminal Analysis Centre shall transfer data from the log system to the National Authority for Data Protection and Freedom of Information and for persons and organisations carrying out activities set out in law for a purpose specified in paragraph (5). The Counter-Terrorism Information and Criminal Analysis Centre shall log also any data provision from the log system.

(7) The Counter-Terrorism Information and Criminal Analysis Centre shall protect the log system from unauthorised access.

(8) In the log system, the retention period of log entries shall be ten years from their creation. Following the expiry of the retention period, the log entry shall be deleted without delay, unless the log entry is required for a pending vetting proceeding. In such a situation, the deletion shall be carried out after the termination of the proceeding.

Secret information gathering

Section 53 (1) With the exception of the Counter-Terrorism Information and Criminal Analysis Centre, national security services may carry out secret information gathering for the performance of their tasks specified in sections 4 to 9; this does not include the performance of tasks specified in sections 4 *h)* and 8 (1) *d)* to *e)*.

(2) National security services may use the special means and methods of secret information gathering only in a case, where the data necessary for the performance of tasks under this Act cannot be obtained in another way.

(3) A national security service authorised to carry out secret information gathering shall carry out secret information gathering individually or with assistance from another national security service, or shall enlist the services of the Special Service for National Security for this purpose.

Secret information gathering not subject to external permission

Section 54 (1) Within the framework of secret information gathering, national security services

a) may request information;

b) may, concealing national security nature, gather information;

c) may establish secret contacts with private persons;

d) may establish and use information systems facilitating information gathering;

e) may use traps not causing any injury and damage to health;

f) may create and use cover documents, cover deeds and cover data to protect their own personnel and the private persons cooperating with them, and to conceal national security nature;

g) may establish and maintain cover institutions;

h) may covertly surveil a person relevant to their tasks, a related home, other premises or fenced area, a public place or a place open to public, or a vehicle; may gather information about the events, and may record, using technical means, the things observed;

i) with the exceptions specified in section 56, may intercept conversations, and may record, using technical means, the things observed;

j) may obtain data necessary for ascertaining the fact of communication through an electronic communications device or information system, for identifying the electronic communications device or information system, or for determining their location.

(1a) For the performance of tasks specified in paragraph (1) *f)* and *g)*, national security services may enter, or have, within the framework of cooperation under this Act, the authorised state organ enter, data in registers specified in section 41 (1). If data is entered, on the basis of a request by a national security service, by another state organ, the requesting national security organ shall be responsible for the lawfulness of data entry.

(2) A law enforcement organ, the Military National Security Service, the Parliamentary Guard and the organ of the National Tax and Customs Administration acting as an investigating authority may be used as a cover institution, or their documents as cover documents, cover data or cover deeds, only if the competent Minister and the national head of the organisation concerned, and regarding the Parliamentary Guard, the commander and the Speaker of the National Assembly, are informed of the fact.

Section 55 (1) Upon permission by a prosecutor designated by the Prosecutor General, national security services may conclude an agreement with the perpetrator of a criminal offence, in which they propose not to initiate a criminal proceeding, or to terminate a pending criminal proceeding, against that perpetrator, if the national security interest for cooperation with the person concerned is more significant than the State interest in enforcing criminal justice.

(2) No agreement shall be concluded, if criminal proceedings are to be carried out against a perpetrator relating to a criminal offence intentionally causing the death of another person, permanent disability or serious degradation of health. The agreement shall be rescinded if national security services become aware of the fact that the person providing information committed such a criminal offence.

(3) If the perpetrator of the criminal offence complies with the provisions of the agreement, criminal proceeding shall not be launched against him; or the criminal proceeding pending against him shall be terminated.

(4) The Counter-Terrorism Information and Criminal Analysis Centre and, with the exception of the task under section 8 (1) *i)*, the Special Service for National Security shall not have the right specified in paragraph (1).

(5) If a criminal proceeding is not launched against the perpetrator, or the criminal proceeding pending against him is terminated, due to his compliance with the agreement, and he fails to pay the damages or the grievance award he is liable to under civil law, such damages or grievance award shall be paid by the State. To ensure the payment of compensation for damage, or a grievance award, the national security services may initiate the conclusion of a confidentiality agreement with the aggrieved party and may prepare the documents required.

(6) If the payment of damages or a grievance award is to be adjudicated in civil proceedings, the legal basis of such claim shall be presumed. The State is represented in the civil proceedings by the Minister responsible for justice. Before adjudicating the claim, the court proceeding in the civil proceedings shall obtain a statement by the national security service about the act committed against the plaintiff and the damage, or violation of personality rights, caused by this act. The statement shall not include any facts based on which conclusions may be drawn regarding a person cooperating in secret.

Secret information gathering subject to external permission

Section 56 Based on an external permission, national security services

a) with the exception of public places and places open to public, may secretly search a home, other premises, fenced area or, with the exception of means of public transport, a vehicle, and objects used by the person concerned, and may record, using technical means, the things observed,

b) with the exception of public places and places open to public, may secretly surveil and record, using technical means, events in a home, other premises, fenced area or, with the exception of means of public transport, a vehicle, and may place the technical means necessary for this at the place of operation,

c) may secretly open a postal item or other sealed consignment linked to an identifiable person and intercept, verify and record its content,

d) may secretly intercept and record the content of communications conducted through an electronic communications network or device using an electronic communications service, or through an information system,

e) may secretly gain knowledge of data processed in an information system, record, using technical means, the things observed, enter the necessary electronic data in the information system, place the necessary technical means, with the exception of public places and places open to public, in a home, other premises, fenced area, or with the exception of means of public transport, a vehicle or an object used by the person concerned, and interfere with an information system to avert a cyber threat.

Section 57 (1) A submission for permission for secret information gathering under section 56 may be filed by the director-general of the Information Office, the Constitution Protection Office, the Military National Security Service and, regarding the performance of the task specified in section 8 (1) *f)*, the Special Service for National Security.

(2) The submission shall contain

a) the place of secret information gathering, the name of the person or persons concerned, or the scope of such persons, and the available data suitable for identification;

b) the specification of secret information gathering and the justification for its necessity;

c) the starting day and the last day of the activity;

d) with respect to a submission for permission under section 59, the reasons for which it was strictly necessary for the effective operation of the national security service in the specific case.

Section 58 (1) In the course of the performance of national security tasks specified in sections 5 *b), d), h)* to *j)* and 6 *d), i), l)* to *n)*, the secret information gathering under section 56 shall be permitted by a judge designated for this task by the president of the Budapest-Capital Regional Court.

(2) In the course of the performance of national security tasks not falling within the scope of paragraph (1), secret information gathering under section 56 shall be permitted by the Minister responsible for justice.

(3) The judge and the Minister responsible for justice (hereinafter jointly "permitting officer") shall adopt a decision within 72 hours after filing the submission. He shall uphold or dismiss, as unfounded, the submission. No appeal shall be accepted against this decision.

(4) Unless otherwise provided in this Act, the permitting officer shall permit secret information gathering for no longer than 90 days at a time. Unless otherwise provided in this Act, in justified cases, the permitting officer may extend this time limit by another 90 days upon a submission by a director-general.

(5) When making a decision regarding an extension of the time limit, the judge may consult data obtained and recorded in the course of secret information gathering permitted by him in the specific case.

(6) The permitting officer shall not inform the persons concerned of its proceedings or of the fact of secret information gathering.

(7) Before initiating criminal proceedings, the head of an organ carrying out secret information gathering shall provide for obtaining a certificate under section 257 (2) of Act XC of 2017 on the Code of Criminal Procedure (hereinafter the "Code of Criminal Procedure"). The president of the regional court shall issue, within three working days after the receipt of an application for it, a certificate under section 257 (2) of the Code of Criminal Procedure that shall be sent to the organ entitled to initiate criminal proceedings by the head of the organ carrying out secret information gathering.

Exceptional permission

Section 59 (1) The directors-general of national security services may grant permission for carrying out secret information gathering under section 56 for no longer than until a decision is made by the permitting officer, if the procedure for obtaining external permission for secret information gathering would cause a delay obviously harming the interest in the effective operation of national security services regarding the case concerned.

(2) In a case specified in paragraph (1), directors-general shall file a submission for external permission concurrently with the grant of their permission.

(3) Secret information gathering upon exceptional permission under paragraph (1) may only be ordered once in a specific case, unless a new fact directly threatening national security arises.

Termination of secret information gathering subject to external permission

Section 60 (1) Secret information gathering subject to external permission shall be terminated without delay if

a) it reached its purpose set out in the permission;

b) no results can be expected from its further application;

c) its time limit expired without being extended;

d) the secret information gathering is unlawful for any reason.

(2) With respect to exceptional proceedings specified in section 59 (1), secret information gathering shall also be terminated without delay if secret information gathering is not permitted by the permitting officer. In such a case, data obtained in the course of secret information gathering shall be destroyed without delay in accordance with provisions of law on the destruction of classified data.

Miscellaneous rules on secret information gathering and the use of covert means

Section 61 (1) If secret information gathering or the use of covert means is performed in accordance with section 8 (1) *a)*, the requesting organ shall be responsible for obtaining permission for secret information gathering or for using covert means. For the lawfulness of their use, the requesting organ, while for their performance, the Special Service for National Security shall be responsible.

(2) The Special Service for National Security shall transfer all data obtained as a result of secret information gathering performed within the framework of its service tasks, or of using covert means, only to the organ issuing an order for such; the transferred data shall be deleted from the records of the Special Service for National Security.

(3) The Special Service for National Security shall keep records regarding its service tasks, which contains:

a) the written request from the ordering organisation, with the permission required,

b) the personal data necessary for identifying the persons specified in the request,

c) a description of the means and methods applied in the course of secret information gathering or using covert means; and information or technical data with operational value that does not qualify as personal data,

d) the list of data-storage media handed over to the ordering organisation.

(4) The data provider shall be responsible for the authenticity of data provided; while the organ ordering secret information gathering, or the implementation of using covert means, shall be responsible for taking or omitting measures on the basis thereof.

(5) The Special Service for National Security shall not store personal data, other than those referred to in paragraph (3), in connection with the performance of its service tasks.

Section 62 Natural persons, legal persons or organisations without legal personality cooperating with a national security service shall not publicly disclose data connected to this activity without permission of the Minister or the director-general.

Section 62/A An organ authorised to engage in secret information gathering, or in the use of covert means, not covered by this Act may use the means of secret surveillance of an information system exclusively by enlisting the services of the Special Service for National Security.

Special rules on financial management related to secret service activities

Section 63 (1) National security services may include appropriations in their budget to cover expenditures on special operations connected to their core activities. In derogation of the general rules on accounting, special operational expenditures shall be featured as a single aggregate amount.

(2) Personal and material expenditures directly associated with the secret service activities of national security services, and with the use of means and methods of secret information gathering, shall be considered as special operational expenditures.

(3) From the amount paid by the national security services to a cooperating private person a withholding tax of 20% shall be deducted and paid to the tax authority. This income need not be declared by, or included in the consolidated tax base of, the private person; the paying national security service need not provide personalised data, or issue a certificate to the private person, regarding this amount.

(4) From income paid to a member of the professional personnel of a national security service for a foreign mission, tax shall be deducted and paid to the tax authority, applying the highest tax rate in the tax scale for the year concerned. This income need not be declared by, or included in the consolidated tax base of, the private person, the paying national security service need not provide personalised data, or issue a certificate to the private person, regarding this amount.

(5) National security services shall exercise the totality of ownership rights and obligations of the State over assets directly related to, and obtained and used for the purpose of, the secret service activities of the national security services and the application of means and methods of secret information gathering.

(6) The income from sale of assets related to the secret service activities of national security services and to the application of means and methods of secret information gathering shall be the special income of national security services, which shall be used for the purchase, refurbishment, installation or extension of real estate or other equipment necessary for this activity.

Section 64 (1) For the performance of their tasks, national security services may establish and maintain cover institutions in accordance with the provisions of law on the type of the institution used as cover. Budgetary organs shall not be established as cover institutions.

(2) The establishment and maintenance of cover institutions shall be financed from the budget of national security services. The expenditure required shall be considered special operational expenditure.

(3) If a cover institution ceases to exist, the national security services shall be entitled to its assets.

(4) The provisions of the Act on public finances shall not apply to cover undertakings.

Section 65 Within the scope provided for in section 63 (2), national security services may handle currency without further restrictions.

Section 66 (1) The supervision, by an external organ, of the use of special operational expenditure by national security services shall only extend to the lawfulness thereof. With the exception of section 11 (2) *f)*, no supervision shall be exercised based on the aspects of expediency and efficiency in this regard.

(2) In the course of supervision, by an external organ, of the financial management of national security services, the organ exercising supervision shall not obtain any data referring to any information generated in the course of secret information gathering, to the source thereof, and to the exact nature of the method used for secret information gathering.

Rules of national security protection and vetting

Section 67 (1) The purpose of national security protection provided by national security services (hereinafter "protection") is to detect, and ward off, covert endeavours directed against the activity of persons specified in Annex 1 or aimed at the unlawful acquisition of protected information related to the activities of these persons and thereby interfering with, or threatening, the national security interests of Hungary.

(2) In the course of providing protection, national security services may use the means and methods of secret and open information gathering regarding a person to be protected, only with his written consent.

(3) National security service shall regularly inform the persons to be protected of security measures taken in the course of providing protection and of the scope of persons affected by these measures.

Section 68 (1) The purpose of national security vetting performed by national security services shall be to examine whether a national security risk can be identified regarding a person subject to national security vetting in connection with security conditions necessary for the lawful operation of State structure and national economy or, where appropriate, arising from international commitments.

(2) A risk to national security shall arise concerning a person subject to national security vetting if

a) there are circumstances rendering him unfit for the lawful performance, without undue influence, of the legal relationship underlying national security vetting, or

b) there are circumstances related to his personal situation that interfere with, or threaten, the interest in the protection of classified information.

Section 69 (1) Persons subject to national security vetting shall be specified in section 74 *i)*.

(2) Within the scope set out in section 74 *i) in)* and *io)*, positions, jobs, offices and posts (hereinafter jointly "position") subject to national security vetting shall be specified

a) with respect to organs under the direction of the Government, in a decree issued by the Minister exercising direction and supervision, with consent of the Minister responsible for the direction of the national security service having the powers to conduct national security vetting,

b) with respect to employing organisations not directed by the Government, in a public law regulatory instrument issued by the head of the employing organisation with consent of the Minister responsible for the direction of national security services having the powers to conduct national security vetting or, if he is not entitled to issue such, in a written measure by the employer approved by the Minister responsible for the direction of national security services having the powers to conduct national security vetting.

Section 70 (1) Unless otherwise provided in this Act, the person entitled to establish a legal relationship underlying national security vetting shall initiate the vetting of a person subject to national security vetting prior to the establishment of the legal relationship underlying national security vetting. The person exercising employer's rights shall initiate the national security vetting of a judicial employee employed by a judicial organ. The Prosecutor General shall initiate the national security vetting of a person in a prosecution service relationship.

(2) In derogation of paragraph (1), the following persons shall be entitled to initiate national security vetting:

a) the President of the Republic, regarding persons specified in section 74 *i) if)* and *ig)*,

b) the Speaker of the National Assembly, regarding persons specified in section 74 *i) ie), il), im)* and *iv)*, and from among the persons specified in section 74 *i) iu)*, regarding members of the professional personnel of the Parliamentary Guard who hold the rank of general, or are in positions with the rank of general,

c) the Prime Minister, regarding persons specified in section 74 *i) ib)* and, with the exception of persons referred to in point *h)*, section 74 *i) id)*,

d) the Minister responsible for the direction of the activity, regarding persons specified section 74 *i) ia), ic), ih)* and *ii)*,

e) the Minister exercising ownership rights on behalf of the State or the person designated to exercise ownership rights on the basis of section 7/A (1) of Act CXCVI of 2011 on national assets, regarding persons specified in section 74 *i) ij)* and *it)*,

f) the director-general competent regarding the personnel, in the case specified in section 74 *i) ik)*,

g) the commander of the Parliamentary Guard, regarding persons specified in section 74 *i) iu)*.

h) the Minister responsible for direction according to the activity concerned, regarding the head and deputy head of a central agency the competence of which does not extend to the entire country from the persons referred to in section 74 *i) id)*.

(3) The head of the National Security Authority shall initiate the national security vetting of persons subject to national security vetting if the person entitled to initiate it cannot be determined based on paragraphs (1) to (2).

(4) The national security vetting of the following need not be initiated:

a) the President of the Republic,

b) the Prime Minister,

c) members of the Constitutional Court,

d) the Speaker of the National Assembly,

e) the President of the Curia, the President of the National Office for the Judiciary,

f) the Prosecutor General,

g) the Commissioner for Fundamental Rights and his deputies,

h) the President of the National Authority for Data Protection and Freedom of Information,

i) Members of the European Parliament elected in Hungary and, unless otherwise provided in this Act, the Members of the National Assembly, and

j) national minority advocates.

(5) Furthermore, national security vetting need not be initiated regarding persons specified in section 74 *i)* who are entitled, under an Act, to access, or use, classified data without national security vetting.

Section 71 (1) Unless otherwise provided in this Act, legal relationships underlying national security vetting may be established only after national security vetting is performed, provided that the national security vetting did not identify any national security risks.

(2) Legal relationships underlying national security vetting may also be established before national security vetting is performed if doing so is approved by any of the following:

a) a person or body directing or supervising the person or body entitled to enter into a legal relationship subject to national security vetting,

b) the Speaker of the National Assembly, regarding a person specified in section 70 (2) *g)*,

c) the Prime Minister, regarding a person specified in section 70 (2) *c), d)* or *e)*,

d) the Minister responsible for the direction of a national security service managed by the director-general with competence over the personnel, regarding a person specified in section 70 (2) *f)*,

e) an executive judicial officer with the power of appointment over the person exercising employer's rights, or in the absence of such, the President of the National Office for the Judiciary, regarding a judicial employee,

f) the Prosecutor General, regarding persons in prosecution service relationship.

(3) In the absence of a person or organ with the right of direction or supervision as set out in paragraph (2) *a)*, the person or body entitled to enter into a legal relationship underlying national security vetting shall decide on establishing the legal relationship based on which national security vetting is required prior to the performance of national security vetting.

(4) If the national security vetting identifies any national security risk, the legal relationship subject to national security vetting may only be established if its establishment is approved by the organ, person or body specified in paragraph (2) or (3).

(4a) If a national security vetting identifies a national security risk in a case under paragraph (2) after the establishment of a legal relationship subject to national security vetting,

a) measures shall be taken to terminate the legal relationship subject to national security vetting with the person exercising employer's rights considering the reassignment of the person concerned to another position or post not subject to national security vetting, or the termination of his occupational relationship, or

b) a legal relationship subject to national security vetting may only be maintained if its maintenance is approved by an organ, person or body specified in paragraph (2) or (3).

(5) In the cases specified in paragraphs (2) to (4a), the person with the right of initiative shall notify of the establishment, or maintenance, of a legal relationship subject to national security vetting the national security service performing national security vetting.

(6) In a case specified in paragraph (4) or (4a), the National Security Authority shall not issue the security clearance required for consulting data to be protected by security verification under an international commitment.

(7) The organ employing a person subject to national security vetting shall inform the national security service with competence to conduct the national security vetting if the person concerned does not occupy a position subject to national security vetting anymore, and as a consequence his legal relationship subject to national security vetting no longer exists.

Conducting national security vetting

Section 71/A (1) National security vetting shall not be conducted without the prior written consent, also covering possible review procedures, of the person subject to national security vetting. If a person subject to national security vetting does not give his consent to the national security vetting, the relationship underlying the national security vetting shall not be established or maintained.

(2) Before the national security vetting is initiated, a person subject to national security vetting may fill in the security questionnaire in Annex *2* in writing or by using the electronic framework program available on the website operated by the national security service affected by the performance of the national security vetting.

(3) During the period of a legal relationship subject to national security vetting, or during the performance of national security vetting, a person subject to national security vetting shall inform, as provided for by a government decree, the national security service of any change in significant data, facts or circumstances from among the data provided in the security questionnaire. The scope of data, facts and circumstances to be considered significant in relation to the security questionnaire, and the detailed rules on the notification obligation regarding any change in significant data, facts or circumstances, and on forwarding the content of such notification to the national security service conducting the national security vetting, shall be set out by the Government in a decree.

(4) A person with the right to initiate national security vetting shall request the national security service in writing to perform the national security vetting.

(5) During the period of a legal relationship subject to national security vetting, the person with the right of initiative shall initiate a new national security vetting no sooner than 180 days and no later than 90 days before the expiry of the valid risk-free security expert opinion.

Section 71/B (1) The director-general of the proceeding national security service shall order the national security vetting within 8 days after the receipt of the initiative. The national security vetting shall be performed within 60 days from the date of it being ordered, which time limit may be extended once for 30 days.

(1a) The director-general shall not order a new national security vetting based on the latter initiative if after a national security vetting of a person was ordered, but before its conclusion, another initiator initiates the performance of national security vetting regarding the same person. If the national security vetting is not ordered, the director-general of the national security service shall notify, in writing, the latter initiator of this fact and of the content of the written notifications previously sent to the other initiator. Subsequently, the latter initiator shall also proceed with the rights of the initiator in the national security vetting pending; the director-general of the national security service shall notify, in writing, both initiators of this fact.

(2) An extension of the time limit of a national security vetting shall be decided upon by the director-general of the proceeding national security service, who shall inform, in writing, the initiator and, through the initiator, the person subjected to national security vetting of this decision within 8 days.

(3) In the course of a national security vetting, risk factors shall be examined and assessed in a manner proportionate to the security requirements for the position requiring national security vetting and for the protection of classified data, and to any other security requirements.

(4) In the course of a national security vetting, the proceeding national security service shall use means that are strictly necessary for conducting national security vetting and that restrict the fundamental rights of the persons concerned to the least possible extent.

(5) In the course of national security vetting, the proceeding national security service may consult the person subjected to the vetting, hear persons associated to him, cross-check data in a security questionnaire with data in records, in data processing systems and data sets, and of previous vetting procedures, and may conduct secret information gathering under this Act.

Section 71/C (1) Based on data and information acquired in the course of the national security vetting, national security services shall prepare a security expert opinion, which shall contain the following:

a) name, mother's name and place and date of birth of the person subject to national security vetting,

b) starting date of the national security vetting,

c) the establishment of a lack of national security risks, or the identification of a national security risk and the reasons for it, and

d) information on the right to legal remedy.

(2) The national security service shall indicate in the security expert opinion the classified data about which the person subjected to national security vetting shall not be informed.

(3) For statements in a security expert opinion, the national security service conducting the national security vetting shall be liable.

(4) If no national security risks were identified during the vetting of a person subject to national security vetting who belongs to the protected personnel of an organ specified in the Act on the police, but it is justified by the nature of an observed circumstance indicating risk, the national security service shall inform of its findings the organ with internal crime prevention and crime detection tasks specified in the Act on the police.

(5) The director-general of the proceeding national security service shall send the security expert opinion to the initiator. If the person subject to national security vetting needs, for the performance of his tasks, to consult data protected by security verification based on an international commitment, the initiator shall forward the security expert opinion to the National Security Authority.

(6) With the exception of circumstances indicating the commission of a criminal offence and of classified data under paragraph (2), the initiator shall, within eight days, inform the person subject to national security vetting of the completion of national security vetting and of the content of the security expert opinion.

(7) A risk-free security expert opinion shall be valid for 5 days from the date of issue.

(8) The former security expert opinion shall become invalid upon the issue of a new security expert opinion prepared based on a new national security vetting conducted within the period of validity of the former risk-free security expert opinion.

(9) If a security expert opinion prepared based on a new national security vetting under paragraph (8) identifies a national security risk after the establishment of a legal relationship subject to national security vetting,

a) measures shall be taken to terminate the legal relationship subject to national security vetting with the person exercising employer's rights considering the reassignment of the person concerned to another position or post not subject to national security vetting, or the termination of his occupational relationship, or

b) a legal relationship subject to national security vetting may only be maintained if its maintenance is approved by an organ, person or body specified in section 71 (2) or (3).

(10) In a case under paragraph (9), the provisions of section 71 (5) and (6) shall apply.

Section 71/D (1) During the period of a relationship underlying national security vetting, a person subject to national security vetting who possesses a valid and risk-free security expert opinion may initiate a review procedure by submitting a reasoned request to the director-general of the national security service entitled to conduct national security vetting.

(2) If a review procedure is requested by a Member of the National Assembly or a person in an occupational relationship with an organisation not directed by the Government or by a Member of the Government, the director-general of the national security service shall, and in any other case he may, order the review procedure initiated in accordance with paragraph (1) within 15 days from the receipt of request.

(3) In a review procedure ordered upon request, the person in a legal relationship subject to national security vetting shall send the filled-in security questionnaire to the director-general of the national security service.

(4) The director-general of the national security service shall inform the person concerned of the completion of the review procedure under section 71/C (5) to (6).

Stay of national security vetting

Section 72 (1) If the effective vetting of a person subjected to national security vetting is rendered disproportionately difficult or impossible by a prolonged stay abroad, a disease or any other external factor outside the control of the national security service conducting national security vetting, the national security vetting shall be stayed until the obstacle ceases to exist.

(2) The director-general of the proceeding national security service shall decide on staying the national security vetting and shall inform, in writing and within 8 days, the initiator and, if it is possible taking into account the reasons for the stay, through the initiator, the persons concerned.

(3) A national security vetting may be stayed until the circumstances for ordering the stay exist, but for no longer than a period of 6 months. If a circumstance giving rise to a stay of national security vetting ceases to exist, the director-general of the proceeding national security service shall order, with simultaneous notification of the initiator and, through the initiator, the persons concerned, the resumption of national security vetting. If the circumstances obstructing national security vetting continue to exist when the time limit for the stay expires, the director-general of the proceeding national security service shall terminate the national security vetting.

(4) The period of the stay of a national security vetting shall not be calculated into the time limit for national security vetting.

Termination of national security vetting

Section 72/A (1) The initiator shall inform, in writing, the director-general of the national security service of the termination of the legal relationship underlying national security vetting of a person subject to national security vetting within 8 days from the date of termination or of becoming aware of it.

(2) The director-general of the national security service conducting national security vetting shall terminate the national security vetting if

a) the initiator informs him of a circumstance serving as ground for termination, or

b) the national security service detects a circumstance serving as ground for termination within its own material competence.

(3) The director-general shall notify the initiator, in writing and within 8 days, of the termination of national security vetting, and the latter shall inform the person subject to national security vetting of this fact without delay.

Review procedure

Section 72/B (1) Within the framework of a review procedure, a national security service may examine

a) a person having a valid and risk-free security expert opinion during the period of the legal relationship underlying national security vetting,

b) a person having a valid and risk-free security expert opinion prior to his nomination for a legal relationship underlying national security vetting, or

c) a person in a legal relationship underlying national security vetting if the establishment, or the maintenance, of the legal relationship was approved under section 71 (2) or (3).

(2) A review procedure may be carried out if

a) the content of the legal relationship of a person in a legal relationship underlying national security vetting, including tasks, rights and obligations related to the position, or the nature of working conditions changes significantly, or there is an increased national security interest in acting in the changed position without undue influence, or if the person in a changed position is more exposed to influence attempts,

b) a person having a valid and risk-free security expert opinion is nominated for a legal relationship underlying national security vetting,

c) a person in a legal relationship underlying national security vetting requests it in accordance with section 71/D,

d) a person in a legal relationship underlying national security vetting failed to perform his notification obligation regarding a change related to national security vetting, or of it is justified due to the nature of the notified change,

e) a person entitled to initiate national security vetting becomes aware of the following relating to a person in a legal relationship underlying national security vetting:

ea) a criminal proceeding, or an infraction proceeding for an infraction punishable by confinement, instituted against the person subjected to vetting or a close relative of such person as set out by the Act on the Civil Code,

eb) an important change to the circumstances, related to foreign persons, organisations or interests, of the person subjected to vetting or the close relative of such person as set out by the Act on the Civil Code,

ec) acquisition of foreign citizenship or foreign passport,

ed) use of drugs, alcohol addiction, behavioural disorders related to alcohol consumption,

ee) high level of indebtedness compared to verified income, significant failure to perform financial obligations, significant enrichment from unknown sources, lifestyle which the verified income cannot cover,

ef) breach of rules on processing classified data or on using security technology systems, and that of security provisions related to holding a position.

eg) maintenance of connections to organised criminal elements, or to a person connected to a rival secret service, by the person subjected to vetting or by a close relative of such person as set out by the Act on the Civil Code,

eh) a change to the lifestyle or circumstances of the person subjected to vetting that may enable influencing or extorting him,

ei) an abuse of official status by the person subjected to vetting,

ej) maintenance of connections to, membership in, or provision of material support to extremist organisations, or groups, of political or religious nature by a person subjected to vetting.

(2a) If the director-general of the national security service having the powers to conduct national security vetting becomes aware of a circumstance indicating a national security risk specified in paragraph (2) *e)*, he may inform the person with the right of initiative about it.

(3) A person with the right to initiate national security vetting may initiate a review procedure under paragraph (2) *a), b)* or *e)* at the director-general of the national security service with material competence to conduct national security vetting. With respect to review procedures initiated under paragraph (2) *a)* or *b)*, before the review procedure is initiated, persons subject to national security vetting shall fill in a security questionnaire in accordance with section 71/A (2), either in writing or by using the electronic framework program specified in section 71/A (2).

(4) The director-general of the national security service having the powers to conduct national security vetting

a) shall order a review procedure if requested by a person with the right of initiative,

b) may order a review procedure if he becomes aware of a circumstance specified in paragraph (2) *a)*, *b)* or *d)*, and

c) shall decide on ordering a review procedure under paragraph (2) *c)*, in accordance with section 71/D (2).

(5) A person subjected to vetting shall be informed of a review procedure ordered under paragraph (2) *d)* or *e)* only after the completion of such review procedure.

(6) A review procedure shall be carried out within 60 days after it is ordered, which time limit may be extended once for 30 days. Section 71/B (2) to (4) shall apply accordingly to review procedures.

(7) Based on a review procedure, the national security service shall issue a security expert opinion, which shall be sent to the initiator. The initiator shall inform, in accordance with section 71/C (6), the persons subject to national security vetting.

(8) In a case specified in paragraph (1) *a)* or *c)*, if the national security service identifies a national security risk in the course of a review procedure, the legal relationship underlying the national security vetting shall be terminated without delay, unless a person, organ or body specified in section 71 (2) or (3) approved the establishment or maintenance of the legal relationship. In order to terminate a legal relationship subject to national security vetting, the person exercising employer's rights shall, at his discretion, provide for

a) either the reassignment of the person concerned to another position or post which is not subject to national security vetting, or

b) the termination of the occupational relationship,

(8a) In a case specified in paragraph (1) *b)*, if the national security service identifies a national security risk in the course of a review procedure, the legal relationship subject to national security vetting, to which the nomination was made, shall not be established regarding the person subjected to national security vetting, unless the establishment of the legal relationship is approved by a person, organ or body specified in section 71 (2) or (3).

(9) The risk-free security expert opinion issued as a result of a review procedure shall be valid for 5 years from the date of issue.

(10) Review procedures shall not be carried out during the period of a national security vetting initiated under section 71/A (5).

Powers of the Commissioner for Fundamental Rights regarding review procedures

Section 72/C (1) Within six months after becoming aware of a review procedure, the person subjected to the review procedure may request the Commissioner for Fundamental Rights to examine the ordering and conduct of the review procedure, to identify irregularities related to fundamental rights.

(2) The Commissioner for Fundamental Rights may carry out an investigation upon a submission under paragraph (1) regarding the ordering and conduct of a review procedure.

(3) The Commissioner for Fundamental Rights may, *ex officio*, examine the practice of national security services relating to review procedures, in order to identify irregularities related to fundamental rights in connection with the ordering and conduct thereof.

(4) The Commissioner for Fundamental Rights may inspect the documents of review procedures as set out in an Act.

(5) The investigative power of the Commissioner for Fundamental Rights shall not cover the professional aspects of identifying national security risks shall not fall under.

(6) If the Commissioner for Fundamental Rights identifies an irregularity related to fundamental rights in the ordering or conduct of a review procedure, he shall notify the Minister responsible for the direction of the national security service and shall, at the same time, make a recommendation for taking the necessary measures. If the violation of law took place within the scope of the tasks of the initiator, the Commissioner for Fundamental Rights shall invite the initiator to take the necessary measures.

(7) The Commissioner for Fundamental Rights shall inform the Committee if he considers the measures taken by the Minister responsible for direction inadequate.

Legal remedy in the course of national security vetting

Section 72/D (1) A person falling under national security vetting may file a complaint with the Minister, through the director-general of the national security service conducting national security vetting, against

a) findings of a security expert opinion which they consider untrue,

b) risk factors identified in a security expert opinion, or

c) a decision that dismisses the ordering of a review procedure initiated by them,

within 15 days after receipt.

(2) The submitted complaint shall have no suspensory effect regarding the termination, under sections 71 (4) or (4a), 71/C (9) or 72/B (8) or (8a), of the legal relationship underlying national security vetting.

(3) If the director-general of the national security service conducting national security vetting agrees with a complaint under paragraph (1),

a) he shall revoke the security expert opinion and issue a new security expert opinion,

b) in a case under paragraph (1) *c)*, he shall order the review procedure.

(4) If the director-general does not agree with a complaint, he shall forward it, together with his position on the matter, to the Minister within 8 days after its submission, and shall, at the same time, inform the person entitled to initiate national security vetting of his decision.

(5) The party with the right of initiative shall inform, without delay, the person subject to national security vetting of the decision of the director-general. The provision of information shall be recorded in minutes, or in another credible way. In the document containing the decision, the person subject to national security vetting shall not be informed of classified information specified by the national security service conducting the national security vetting.

(6) The Minister shall investigate the complaint within 30 days after receipt, which time limit may be extended once for 30 days.

(7) The Minister

a) shall dismiss the complaint, if unfounded, or

b) shall uphold the complaint, and

ba) set aside the decision relating to the identification of a national security risk, and instruct the national security service that conducted the national security vetting to conduct new proceedings,

bb) establish the lack of a national security risk, or

bc) instruct the director-general of the national security service to conduct a review procedure initiated by a person subject to national security vetting if the initiative was dismissed.

(8) The Minister shall inform, in writing, the complainant, the director-general of the national security service entitled to conduct national security vetting and, through the director-general of the national security service, the person with the right of initiative, of a decision under paragraph (7).

(9) A person subject to national security vetting may submit a complaint against a decision by the Minister to the Committee within 15 days of receipt.

(10) If the Committee dismisses the complaint, and the legal relationship of a person subject to national security vetting was terminated based on a security expert opinion identifying a national security risk under sections 71 (4) or (4a), section 71/C (9) or 72/B (8) or (8a), the person subject to national security vetting may challenge the decision by the Minister within 15 days after the receipt of the decision by the Committee. The administrative court action shall be brought against the Minister adjudicating the complaint against the security expert opinion identifying a national security risk. The court action shall fall within the exclusive territorial jurisdiction of Budapest-Capital Regional Court.

(11) A person in a professional service relationship shall also have the right to bring an administrative court action under paragraph (10) if he was dismissed from a post and, simultaneously, placed on non-active status based on a security expert opinion identifying a national security risk.

(12) In an administrative court action under this paragraph, only closed hearings may be held and only judges, whose national security vetting was performed in accordance with this Act, may proceed.

(13) In a proceeding under paragraph (10), the court shall not be entitled to amend a decision pertaining to identifying a national security risk.

(14)

Final provisions

Section 73 If redundancies take place at national security services, the provisions of the Act on the Labour Code on collective redundancies and on the notification of the state employment organ shall not apply.

Interpretative provisions

Section 74 For the purposes of this Act,

a) national security interest means ensuring the sovereignty, and protecting the lawful order, of Hungary, and within this framework,

aa) detecting offensive endeavours against the independence and territorial integrity of the country,

ab) exposing and warding off covert endeavours interfering with, or threatening, the political, economic or national defence interests of the country,

ac) obtaining information related to, or originating from, foreign countries that is necessary for governmental decisions,

ad) detecting and warding off covert endeavours aimed at changing, or disrupting by unlawful means the lawful order of the country ensuring the practice of fundamental human rights, the representative democracy based on a multi-party system, and the operation of legitimate institutions, and

ae) detecting and preventing terrorist acts, illegal drug and arms trafficking and the illegal traffic of internationally controlled products and technologies;

b) state organ means the ministries, the government administration organs, the prosecution service, the Hungarian Defence Forces and the law enforcement organs;

c) information system means a piece of equipment, or the totality of interconnected pieces of equipment, performing the automatic technical processing, processing, storage and transfer of data;

d) single military reconnaissance system means a system providing reconnaissance support to planning and revision of the armed defence of the country and of the defence at alliance level, and to making decisions required for the planning, direction and control of the operations of the Hungarian Defence Forces;

e) relative means the spouse, the lineal relative, the adopted child, the stepchild and the foster child, the adoptive parent, the step-parent and the foster parent, the sibling, the cohabitant, the spouse of a lineal relative, the prospective spouse, the lineal relative and the sibling of the spouse, and the spouse of the sibling;

f) audit of economic operators means audit conducted by a competent national security service aimed at establishing whether assistance, involving the use of classified data, provided by an economic operator constitutes a national security risk;

g) occupational relationship means judicial service relationship, prosecution service relationship, professional service relationship, service relationship of professional or contracted soldiers, public service relationship, government service relationship, tax and customs authority service relationship, public employment relationship, law enforcement administration service relationship, national defence employment relationship, employment relationship and other employment-related relationship;

h)

i) person subject to national security vetting means

ia) a head of a diplomatic mission;

ib) a Minister, a State Secretary, a Government Commissioner, a Prime Ministerial Commissioner and a Prime Ministerial Delegate;

ic) a Permanent State Secretary, a Deputy State Secretary, a Ministerial Commissioner;

id) a head or the deputy head of an autonomous state administration organ, an independent regulatory organ, a central agency, a main government agency, and a capital or county government office;

ie) the Director-General of the Office of the National Assembly, a head and deputy head of a division specified in the organisational and operational regulations of the Office of the National Assembly or those of an autonomous subdivision thereof;

if) the head of the Office of the President of the Republic and a head of an autonomous division of the Office of the President of the Republic;

ig) the commander and deputy commanders of the Hungarian Defence Forces;

ih) the national commander of a law enforcement organ and his deputy, the director-general of the Military National Security Service and his deputy, a chief police commissioner, a police commissioner and a head of a border police office;

ii) a general and a person appointed in a position with the rank of general;

ij) an executive officer, executive employee or member of the supervisory board of a State economic operator or an economic operator under majority State ownership;

ik) the personnel of a national security service, a counter-terrorism organ specified in the Act on the police or an organ performing internal crime prevention and crime detection tasks specified in the Act on the police;

il) a candidate, or member, of the standing committee dealing with national security, or the standing committee dealing with national defence, of the National Assembly or, if the use of data of "bizalmas" ("confidential") or higher classification level is required for the performance of his tasks, of a committee of inquiry, or an *ad hoc* committee, established by the National Assembly;

im) an expert in a proceeding of the standing committee of the National Assembly dealing with national security, or the standing committee dealing with national defence or, if the use of data of "Bizalmas!" ("Confidential") or higher classification level is required for the performance of his tasks, of a committee of inquiry, or an *ad hoc* committee, established by the National Assembly;

in) a person who is in an occupational relationship, or in a contractual relationship under the provisions of the Act on the Civil Code, with an organ processing classified data specified in the Act on the protection of classified data, and is highly exposed to unlawful intentions to influence him, or to covert attacks or threats, in relation to this legal relationship;

io) a person who, based on an occupational relationship, or on a contractual relationship under the provisions of the Act on the Civil Code, is authorised to consult or use data classified as "Bizalmas!" ("Confidential"), "Titkos!" ("Secret") or "Szigorúan titkos!" ("Top secret") under the Act on the protection of classified data;

ip) a natural person cooperating with an organ processing classified data specified in the Act on the protection of classified data, who needs to use data classified as "Bizalmas!" ("Confidential"), "Titkos!" ("Secret") or "Szigorúan titkos!" ("Top secret") for the performance of his tasks;

ir) a judge permitting secret information gathering under this Act;

is) a designated prosecutor specified in section 55;

it) an executive officer, executive employee or member of the supervisory board of a foundation or public foundation over which the founder's rights are exercised by a budgetary organ under the direction or supervision of the Government,

iu) the personnel of the Parliamentary Guard;

iv) a member of the Committee of National Remembrance;

iw) a person participating, on the part of an authority or a specialist authority, in an administrative authority proceeding under the Act on the identification, designation and protection of critical systems and facilities (hereinafter the "Critical Systems Act"), and a cooperating person engaged by the operator, as set out by the Critical Systems Act, in an identification procedure under the Critical Systems Act related to elements of European critical systems;

ix) an employee of the Supervisory Authority of Regulatory Affairs;

iy) an employee of the Hungarian Atomic Energy Authority;

j) analysis and evaluation activity means processing data acquired by national security services to protect the national security and the sovereignty of Hungary, prevent, detect and interrupt the commission of a criminal offence, establish the identity of, and arrest, a perpetrator, search for, and determine the residence of, a wanted person, and obtain evidence; and drawing conclusions from the data processed;

k) cooperating organs means organs specified in section 30/A;

l) air passenger data means data specified in the Act on aviation deriving from a passenger, a person authorised by him, or a service provider selling tickets on behalf of an air carrier transporting passengers;

m) provider of passenger data means an air carrier transporting passengers transmitting, under an Act, data specified in point *l)* for facilitating the prevention, interruption and detection of terrorism and organised crime;

n) direct electronic data link means an information technology application meeting the technical requirements specified by the Counter-Terrorism Information and Criminal Analysis Centre which enables documented data transmission between the Counter-Terrorism Information and Criminal Analysis Centre and a cooperating organ through an interface built by the cooperating organ;

o) watch-listing annotation means a notification order as issued by a national security service, in relation with the performance of its tasks, regarding data processed in data processing systems, which ensures that the national security service issuing the order becomes aware of any event regarding the annotated data, and in particular, changes to, measures taken in relation with, and requests concerning, such data;

p) depersonalisation of air passenger data means making data elements that are suitable for direct identification of the passengers concerned invisible for users through masking out data elements;

q) reinstatement of the suitability for personal identification of air passenger data means reinstating the suitability for personal identification of air passenger data depersonalised through masking out data elements that are suitable for direct identification of the passengers concerned by making masked-out data elements visible;

t) national defence organisation means an organisation as defined in point 13 of section 80 of Act CXIII of 2011 on national defence, the Hungarian Defence Forces and measures applicable during special legal order.

Section 75 (1)

(2)

(3) Where a law refers to a Minister exercising supervisory powers regarding national security services, it shall be understood as the competent Minister responsible for the direction of national security services.

Entry into force

Section 76 (1) With the exceptions specified in paragraphs (2) to (4), this Act shall enter into force on the 90th day after its promulgation.

(2) The provision under section 25 shall enter into force on 1 January 1996.

(3) Sections 63 (3) and 89 (3) shall enter into force on 1 January 1997.

(4) Sections 14 (4) *c)* to *e)*, 15 and 27 (2) and (4) shall enter into force following the establishment of the Committee in accordance with section 19.

(5) Sections 16 (2) and 19 (1) *h)* of Act LXV of 1995 on state secrets and professional secrets shall enter into force on the 90th day after the promulgation of this Act.

Transitional provisions

Section 76/A (1) If a risk-free security expert opinion was issued, regarding a person subject to national security vetting, based on a type "A", "B" or "C" carried out within five years before the establishment of the relationship underlying the national security vetting, after the entry into force of Act LXXII of 2013 amending certain Acts for the purpose of laying down new rules on national security vetting (hereinafter "Amending Act") national security vetting need not be initiated until the 90th day before the expiry of the period of validity of the risk-free security expert opinion.

(2) If before the entry into force of Act CIX of 2014 amending Act CXXV of 1995 on national security services and certain other Acts in connection with national security vetting, a national security vetting was initiated with regard to the time limit until 31 December 2014 set out in section 76/A (1) and (2) *b)* of the Nbtv., such national security vetting shall be carried out in accordance with the provisions of section 71/B of Nbtv., provided that the valid and risk-free national security expert opinion of a person subject to national security vetting was issued by 31 March 2010.

(3) If the valid and risk-free national security expert opinion of a person affected by a national security vetting initiated under paragraph (2) was issued after 31 March 2010, the director-general of the national security service shall request, in writing and within 8 days of the receipt of the initiative, the initiator to make a statement within 15 days whether he maintains his intention to initiate even though the obligation to initiate was terminated. If the initiator abandons the initiative, or fails to make a statement within the time limit, the national security vetting need not be ordered.

Section 76/B The provisions of this Act as introduced by Act CCXXXIX of 2013 amending Act CXXV of 1995 on national security services and Act II of 2012 on infractions, infraction procedure and the infraction records system with a view to making parliamentary monitoring related to national security more effective (hereinafter "Amending Act 2") shall apply also to fact-finding investigations pending on the date of entry into force of the Amending Act 2.

Section 76/C (1) The provisions of this Act as introduced by Act CIX of 2014 amending Act CXXV of 1995 on national security services and certain other Acts in connection with national security vetting (hereinafter "Amending Act 3") shall apply to members to be elected to the Committee on Foreign Affairs of the National Assembly after the entry into force of the Amending Act 3.

(2) With respect to memberships of the Committee on Foreign Affairs of the National Assembly existing at the time of entry into force of the Amending Act 3, the Speaker of the National Assembly shall initiate national security vetting until 28 February 2015.

Section 76/D Cooperating organs shall build the interface for the electronic data link ensuring access to the data processing system of a cooperating organ until 31 December 2016.

Section 76/E (1) The Counter-Terrorism Information and Criminal Analysis Centre shall be the general legal successor of the Coordination Centre Against Organised Crime.

(2) Regarding tasks and competences specified in a law issued prior to the entry into force of Act LXIX of 2016 amending certain Acts in connection with the fight against terrorism, the Counter-Terrorism Information and Criminal Analysis Centre shall be considered as the legal successor of the Coordination Centre Against Organised Crime.

Authorising provisions

Section 77 (1) The Government shall be authorised to determine in a decree:

a) the procedural rules related to filling in the security questionnaire; the scope of data, facts and circumstances which are considered important from the perspective of the security questionnaire specified in Annex 2, and the detailed rules on reporting any changes to these data, facts or circumstances;

b) the scope of security documents, the functions and powers of the organ entitled to security document protection, the procedural rules on security document protection;

c) in order to provide the conditions for secret information gathering or for the use of covert means, the order and rules of cooperation between organs authorised to engage in secret information gathering or to use covert means, and organisations performing electronic communications service tasks;

d) in order to provide the conditions for secret information gathering or the use of covert means, the order and rules of cooperation between organs authorised to engage in secret information gathering or to use covert means, and the application service providers specified in the Act on certain issues of electronic commerce services and information society services.

(2) The Government shall be authorised to determine in a decision:

a) the rules, not laid down in this Act, on the territorial competence of national security services and on their cooperation with each other and with other organs;

b) the main directions for the activities of national security services;

c) the order of information activities of national security services and other state organs, as well as the organisational framework of, and detailed rules on, the assessment and use of national security information;

d) the scope of organs and facilities subject to national security protection.

(3)

Section 78 (1) The Minister shall be authorised to determine in a decree:

a) the order of housing management of national security services, and of employer housing support;

b) the order of employing, and carrying, service weapons and the detailed rules on their use;

c) the order of entry into the facilities of national security services;

d) the order of conferring honours by a Minister.

(1a) With respect to organs falling under their direction or supervision, the Ministers shall be authorised to determine the positions subject to national security vetting in a decree, if conducting the national security vetting falls

a) within the material competence of the Constitution Protection Office, or the Special Service for National Security, in agreement with the Minister responsible for the direction of civilian national security services,

b) within the material competence of the Information Office, in agreement with the Minister responsible for the direction of civilian intelligence activities,

c) within the material competence of the Military National Security Service, in agreement with the Minister responsible for national defence.

(1b) The Minister responsible for the direction of civilian national security services shall be authorised to determine in a decree:

a) the method for communication and data transmission between the Counter-Terrorism Information and Criminal Analysis Centre and the provider of passenger data, and

b) the detailed rules of data provision by the Counter-Terrorism Information and Criminal Analysis Centre to the European Commission, and the scope of statistical data.

(2) The Minister shall be authorised to determine in an instruction:

a) the special conditions for eligibility for service and the rules on verifying eligibility conditions;

b) the general rules of the proceedings of national security services related to the establishment and maintenance of cover institutions;

c) all proceedings which are referred to autonomous regulation by the law on reporting and accounting obligations of budget-based organs;

d) those heads of national security services that are entitled to protection and the detailed rules on protective measures.

(3)The Minister responsible for national defence shall be authorised to determine, in a decree, the companies carrying out activities related to national defence interests, concerning which the Military National Security Service shall perform the tasks under section 6 *a)* to *r)*.

Section 79

Compliance with the requirement of the Fundamental Law on cardinality

Section 79/A The following provisions of this Act qualify as cardinal on the basis of Article 46 (6) of the Fundamental Law:

a) sections 1 to 19/B,

b) sections 26 to 37,

c) sections 53 to 72/D,

d) section 74, and

e) sections 76/A to 78,

f) Annexes 1 and 2.

Compliance with the law of the European Union

Section 80 This Act contains provisions for the implementation of the following legal acts of the European Union:

a) Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime,

b) Article 36 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [section 41/A],

c) Articles 3 to 5 and 16 of Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences [section 11/A, section 45].

Section 81 The prior notification of sections 40 and 41 of this Act was performed in accordance with Articles 5 to 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

Section 82

Section 83

Section 84

Section 85

Section 86

Section 87

Section 88

Section 89

Section 90

Section 91

Annex 1 to Act CXXV of 1995

Offices subject to protection:

1 the President of the Republic,

2 the Prime Minister,

3 the Speaker and the Deputy Speakers of the National Assembly,

4 the President and members of the Constitutional Court,

5 the President of the Curia and its deputies,

6 Ministers,

7 the Prosecutor General and his deputies,

8 the President and Vice Presidents of the State Audit Office of Hungary,

9 the Commissioner for Fundamental Rights and his deputies,

10 members of the Committee on National Security and the Committee on National Defence of the National Assembly,

11 judges permitting secret information gathering,

12 prosecutors designated by the Prosecutor General under section 55,

13 the Governor and Deputy Governors of the Hungarian National Bank,

14 the President and Vice Presidents of the Hungarian Competition Authority,

15 the President and Vice President of the National Authority for Data Protection and Freedom of Information.

Annex 2 to Act CXXV of 1995

SECURITY QUESTIONNAIRE

for security vetting of persons subject to national security vetting

I General personal data	
1	Family name and given name:
2	Name at birth:
3	Place, year, month and day of birth:
4	Mother's name:
5	Identity card number:
6	Contact details (phone number, email address):
II Data on citizenship	
1	Current citizenship:
2	Former citizenship (indication of the state, date and document number):
3	In the case of foreign or dual citizenship:
4	beginning date of the stay in Hungary:
5	legal title and status:
6	number and issue date of residence permit, name of issuing authority:
7	passport number:
8	name of the authority processing the application for permanent residence or immigration:
9	submission date of application for naturalisation or citizenship, name of proceeding authority:
III Data on marital status and relatives	
1	Marital status: married man, single man, married woman, single woman, divorced person, person living in cohabitation, widowed person (please underline the appropriate term)
2	The current spouse's or partner's
3	family name and given name:
4	name at birth:
5	place, year, month and day of birth:
6	mother's name:
7	citizenship (See points II 1 to 3):
8	occupation and position:
9	name and address of workplace:
10	Personal data of children:
11	family name and given name:
12	name at birth:
13	place, year, month and day of birth:
14	mother's name:
15	citizenship (See points II 1 to 3):
16	occupation and position:
17	name and address of workplace:
17a	Personal data of parents
17b	family name and given name:
17c	name at birth:

17d	place, year, month and day of birth:
17e	mother's name:
17f	citizenship (See points II 1 to 3):
17g	occupation and position:
17h	name and address of workplace:
18	Data of persons over the age of 18 not listed above, living in the same household with you:
19	family name and given name:
20	name at birth:
21	place, year, month and day of birth:
22	mother's name:
23	citizenship (See points II 1 to 3):
24	occupation and position:
25	name and address of workplace:
26	Your relatives, and the relatives of your spouse or partner, living abroad:
27	family name and given name:
27a	name at birth:
27b	mother's name at birth:
28	place, year, month and day of birth:
29	address:
30	occupation and position:
31	citizenship:
32	degree of blood relationship:
IV Data on address and residence	
1	Your address:
2	Your place of residence:
3	Former addresses and places of residence where you stayed for more than 3 months (in the past 15 years):
4	If you stayed abroad for more than 6 months, please indicate the address abroad and the reason for the stay (in the past 15 years):
V Data on educational qualifications	
1	List the educational institutions from secondary school onwards where you studied as a student (name and the address of the educational institution, duration of training, date of completion; certificate number and date of issue of documents certifying education or training):
2	With respect to studies abroad, name and address of the educational institution, duration of training, date of completion; certificate number and date of issue of documents certifying education or training:
3	Academic degree (where, when and regarding what subject was it obtained):
4	Professional, scientific publications (title, place and time of publication, the subject concerned):
5	Foreign language proficiencies and their level:

VI Occupational data	
1	Current occupation, post, name and address of employer:
2	Former occupation, post and positions, with date (in the past 15 years), and the name and address of employers:
VII Data on military service	
1	Did you serve in the military (when, where, special military training):
VIII Data related to the income and financial situation of you, your spouse or your cohabitant	
1	Gross annual income from main occupation:
2	Sources of income exceeding gross HUF 500 000 per annum, other than your main occupation:
3	Debts or financial liabilities owed to tax authority, social security or financial institutions in the past 5 years:
4	Do you have any interest in an economic operator registered at a domestic company registration court:
5	name and address of such economic operators, the scope of their activities:
6	The nature of such interest (owner, co-owner, member of the management board, supervisory board member, etc.)
7	Do you have any official relation with economic operators registered abroad, and the nature of the cooperation or relation:
8	name and address of the economic operators:
9	their scope of activities:
10	place of their registration
11	Were you or your companies subject to enforcement proceedings in the past 15 years? (If yes, please provide details: when, why, name of the ordering court or authority):
IX Assets of you and your relatives living in the same household with you:	
1	The owned real estate's
2	address and parcel identification number:
3	surface area:
4	ownership proportion:
5	time and title of acquisition:
6	Movable property owned, with a value exceeding HUF one million:
7	motor vehicles (type, license plate number):
8	protected work of art, protected collection (creator, title, registration number):
9	other movable property (name, time and title of acquisition):
9a	Amount of cash savings:
10	Savings in securities under point 34 of section 3 of Act CXVII of 1995 on personal income tax:
11	designation:
12	serial number:
13	amount:
14	Claim arising from bank deposit or savings deposit contracts under the Civil Code.

15	name of credit institution:
16	account number or deposit book number:
17	amount:
18	Debts owed to domestic financial institutions or financial institutions registered abroad
19	name of financial institution:
20	account number:
21	amount:
21a	Claims against financial institutions registered abroad
21b	name of financial institution:
21c	account number:
21d	amount:
21e	Savings with building societies
21f	name of building society:
21g	amount of savings:
21h	Retirement savings (pension insurance, pension savings account, voluntary pension fund):
21i	name of financial institution or insurance institution:
21j	account number (if applicable):
21k	amount:
22	Income from abroad
23	its source:
24	its amount:
25	its title:
26	date of its realisation:
X Data on criminal and infraction proceedings	
1	Were you or your spouse (cohabitant) subject to a criminal proceeding, within 15 years before the date of the completion of this questionnaire, that resulted in a punishment (If yes, please provide details: when, why, name of proceeding court, extent of punishment, and the date of expungement):
2	Were you or your spouse (cohabitant) subject to an infringement or disciplinary proceeding, within 5 years before the date of the completion of this questionnaire, that resulted in a punishment (If yes, with the exception of traffic infractions, please provide details: when, why, name of proceeding authority, extent of punishment):
3	Are you or your spouse (cohabitant) subject to a pending criminal, infraction or disciplinary proceeding, or involved in a case for damages (If yes, with the exception of traffic infractions, please provide details: why, name of proceeding court or authority):
XI Special data	
1	When employed in Hungary or abroad, did you work in a position which required the filling-in of a security questionnaire or a security statement before commencement (If yes, please indicate the workplace, the name of the post and the date thereof):
2	Have you ever observed any circumstance during your career based on which the presence of a foreign intelligence service may be inferred (attempts at establishing relationships, recruiting or compromising) If yes, please provide details:
3	Have foreign authorities taken measures for expulsion, or prohibition of entry or stay,

	against you or your close relative in the past 5 years; or are you currently subject to such measures? (If yes, please indicate the measure, the ordering authority and the date of the measure.)
XII Regarding you, your spouse or cohabitant:	
1	What is the extent of your private contact with foreign nationals? Specify the most important contacts, but not more than 15 persons:
2	family name and given name:
3	place, year, month and day of birth:
4	address:
5	occupation and workplace:
6	citizenship:
7	nature and short description of contact:
8	Do you maintain, or did you ever maintain, contact with a person who to your knowledge is, or was, a member of the personnel of a foreign intelligence service or a cover institution thereof? (If yes, please provide details.)
9	Do you drink alcohol? If yes, to what extent:
10	have you ever suffered from alcohol dependence?
11	have you ever taken part in treatment for alcoholism?
12	Have you ever occasionally, or regularly, consumed, distributed or produced drugs or narcotic or intoxicating substances or medicinal products; when, to what extent, and what type?
13	Do you have a relationship outside marriage or cohabitation (including same-sex relationships)?
13a	family name and given name of the partner:
13b	name at birth of the partner:
13c	the partner's place, year, month and day of birth:
13d	name of the partner's mother:
14	Are you, or were you, in contact with (fascist, Arrow Cross, communist, anarchist or other extremist) organisations, movements, groups, etc. denying the legal principles of the democratic rule-of-law state, or carrying out activities of nature? (If yes, please provide details):
15	In addition to the above, are you aware of any circumstance (risk factor) the reporting of which you consider necessary from the perspective of security vetting (e.g. information suitable for compromising or blackmailing)?
16	You may specify reference persons (no more than 3 persons) who can give objective opinion on you and with whom you are not in a family relationship or a dependent relationship:
17	name, address and phone number:
18	since when have you known each other:

XIII. SECURITY STATEMENT

I hereby declare that the data provided by me are true and correct.

I hereby give consent for the national security service conducting national security vetting to gather data regarding my person, and to verify, within the framework of national security

vetting, the fulfilment of security requirements prior to the establishment of a legal relationship underlying national security vetting, and to verify, within the framework of a review procedure, the fulfilment of such requirements during the period of that legal relationship. I acknowledge that if the data cannot be obtained in any other way, the national security service conducting national security vetting may also carry out secret information gathering regarding my person.

When filling in the questionnaire, I was aware that I am not obliged to provide answers to questions that would accuse me or my relatives of committing a criminal offence or an infringement.

Done at ....., …… 201.....

signature, address

XIV Statement of a spouse, registered partner, cohabitant or adult relative living in the same household

I hereby acknowledge that the national security vetting, including checks related to a change in data, of my spouse, cohabitant or adult relative living in the same household may concern also my person; in this framework, if the data necessary cannot be obtained in any other way, the national security service conducting national security vetting may also carry out secret information gathering.

Done at ....., ……201..

signature, address

Annex 3 to Act CXXV of 1995

Criminal offences qualifying as terrorist and serious criminal offences for the purpose of receiving and processing passenger data

1. 1 Terrorist criminal offences:

1.1 terrorist offences under Article 1, offences relating to a terrorist group under Article 2, offences linked to terrorist activities under Article 3 or inciting, aiding or abetting, and attempting an offence under Article 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism,

1.2 changing the constitutional order by force [section 254 (1) and (2) of the Criminal Code],

1.3 conspiracy against the constitutional order [section 255 (1) and (2) of the Criminal Code],

1.4 terrorist act [sections 314 (1) and (2), 315 (1) and (2), 316 and 316/A of the Criminal Code],

1.5 terrorism financing [sections 318 and 318/A of the Criminal Code]

1.6 incitement to war [section 331 of the Criminal Code]

2. 2 Serious criminal offences:

2.1 crimes against humanity [Chapter XIII of the Criminal Code],

2.2 war crimes [Chapter XIV of the Criminal Code],

2.3 homicide [section 160 (1) to (3) and (5) of the Criminal Code],

2.4 homicide in the heat of passion [section 161 of the Criminal Code],

2.5 causing grievous bodily harm [section 164 (3), (6) and (8) of the Criminal Code],

2.6 illegal use of a human body [section 175 (1) to (3) of the Criminal Code],

2.7 drug trafficking [sections 176 (1) to (4), (5) b *b)*, (6) and 177 (1) *b)*, *c) cb)* and (2) to (5) of the Criminal Code],

2.8 abuse of drug precursors [section 183 (1) *a)* of the Criminal Code],

2.9 abuse of new psychoactive substances [sections 184 (1) to (3), 184/A (1) *b)*, *c) cb)*, (2) and (3), 184/B (1) to (3) and 184/C (1) to (3) of the Criminal Code]
2.10 abuse of performance-enhancing substance [section 185 (1) *a)* and *b)*, (2) and (3) of the Criminal Code],
2.11 counterfeiting of medicinal products [section 185/A (1) to (6) of the Criminal Code]
2.12 counterfeiting of medical products [section 186 (1) to (4) of the Criminal Code],
2.13 kidnapping [section 190 (1) to (5) of the Criminal Code],
2.14 failure to report kidnapping [section 191 of the Criminal Code],
2.15 trafficking in human beings and forced labour [section 192 (1) to (6) of the Criminal Code],
2.16 violation of personal freedom [section 194 of the Criminal Code],
2.17 sexual coercion [section 196 (1) to (3) of the Criminal Code],
2.18 sexual violence [section 197 (1) to (5) of the Criminal Code],
2.19 sexual abuse [section 198 (1) to (4) of the Criminal Code],
2.20 procuring [section 200 of the Criminal Code],
2.21 facilitating prostitution [section 201 (1) *c)* and (2) of the Criminal Code],
2.22 exploitation of child prostitution [section 203 of the Criminal Code],
2.23 child pornography [section 204 (1) to (5) of the Criminal Code],
2.24 indecent exposure [section 205 (2) of the Criminal Code],
2.25 damaging the environment [section 241 (1) and alternative III in section 241 (2) of the Criminal Code],
2.26 damaging natural values [sections 242 (1) and (2), and 243 (1) and (2) of the Criminal Code],
2.27 violation of waste management regulations [section 248 (1) and (2) of the Criminal Code],
2.28 abuse of ozone depleting substances [section 249 (1) of the Criminal Code],
2.29 abuse of radioactive materials [section 250 (1) *a)* and *b)*, and (2) to (3) of the Criminal Code],
2.30 riot [section 256 (1) to (3) of the Criminal Code],
2.31 destruction [section 257 of the Criminal Code],
2.32 espionage [section 261 (1) to (3) of the Criminal Code],
2.33 espionage against the institutions of the European Union [section 261/A of the Criminal Code],
2.34 espionage against allied armed forces [section 262 of the Criminal Code]
2.35 active bribery [section 290 (1) to (4) of the Criminal Code],
2.36 passive bribery [section 291 (1) to (4) of the Criminal Code],
2.37 active bribery regarding a public officer [section 293 (1) to (4) of the Criminal Code],
2.38 passive bribery regarding a public officer [section 294 (1) to (4) of the Criminal Code],
2.39 active bribery in a court or in authority proceedings [section 295 (1) and (2) of the Criminal Code],
2.40 passive bribery in a court or in authority proceedings [section 296 (1) and (2) of the Criminal Code],
2.41 active trading in influence [section 298 (1), (1a) and (3) of the Criminal Code],
2.42 passive trading in influence [section 299 (1), (2), (4) and (5) of the Criminal Code],
2.43 failure to report a corruption criminal offence [section 300 (1) of the Criminal Code],
2.44 unlawful seizure of a vehicle [section 320 (1) to (3) of the Criminal Code],
2.45 participation in a criminal organisation [section 321 (1) of the Criminal Code],

2.46 disturbing the operation of public interest enterprises [section 323 (1) to (3) and (5) of the Criminal Code],
2.47 abuse of explosives or detonating equipment [section 324 (1), (2) and (3) of the Criminal Code],
2.48 abuse of firearms or ammunition [section 325 (1) *b)* and *c)*, (2) *b)* and *c)*, (3) and (5) of the Criminal Code],
2.49 abuse of a weapon prohibited by an international treaty [section 326 (1) to (6) of the Criminal Code],
2.50 violation of an international economic restriction [section 327 (1) to (4) of the Criminal Code],
2.51 abuse of military products or services [section 329 (1) to (4) of the Criminal Code],
2.52 abuse of dual-use products [section 330 (1) and (2) of the Criminal Code],
2.53 public deed forgery [sections 342 (1) and 343 (1) of the Criminal Code],
2.54 abuse of unique identification mark [section 347 (1) to (2) of the Criminal Code],
2.55 people smuggling [section 353 of the Criminal Code],
2.56 abuse of protected cultural goods [section 358 (1) *a)* and *c)* and (2) of the Criminal Code],
2.57 robbery [section 365 (3) *a)* to *d)* and (4) *b)* and *c)* of the Criminal Code],
2.58 embezzlement [section 372 (3) *c)* of the Criminal Code],
2.59 fraud [section 373 (3) to (6) of the Criminal Code],
2.60 economic fraud [section 374 (3) to (6) of the Criminal Code],
2.61 information system fraud [section 375 (1) to (5) of the Criminal Code],
2.62 handling stolen goods [section 379 (1) and (3) to (6) of the Criminal Code as in force until 31 December 2020],
2.63 intellectual property infringement [section 384 (1) of the Criminal Code]
2.64 violation of copyright or related rights [section 385 (3) and (4)]
2.65 circumventing technical measures protecting intellectual property [section 386 (3) of the Criminal Code]
2.66 violation of industrial property rights [section 388 (2) and (3) of the Criminal Code]
2.67 money counterfeiting [section 389 (1) to (3) of the Criminal Code],
2.68 facilitating money counterfeiting [section 390 (2) of the Criminal Code],
2.69 budget fraud [section 396 (2) to (7) of the Criminal Code],
2.70 money laundering [sections 399 (1) to (7) and 400 (2) of the Criminal Code],
2.71 placing pour-quality products on the market [section 415 (1) and (2) of the Criminal Code],
2.72 false certification of conformity [section 416 (1) and (2) of the Criminal Code],
2.73 illegal data acquisition [section 422 (1) *d)* and *e)*, (1a) *b)* and (4) of the Criminal Code],
2.74 violation of information systems or related data breach [section 423 (2) to (4) of the Criminal Code].