

Copyright 1999 Polish News Bulletin
5 May 1999
SECTION: Law Supplement
LENGTH: 5072 words

HEADLINE: THE CLASSIFIED INFORMATION PROTECTION ACT of 22 January
1999 (Part I)

BODY: CHAPTER 1 COMMON PROVISIONS

Article 1.

1. This Act defines the standards and requirements for safeguarding information expressed in whatever form and manner, including information in the course of development, which must be protected against unauthorised disclosure because it is a state secret or public service secret, hereinafter called "classified information", and specifically concerning:

- 1) organising the protection of classified information;
- 2) the classified information rating system;
- 3) the access to classified information;
- 4) the investigative proceeding conducted with a view to establishing whether the person under review is fit and proper to keep secrets, hereinafter called the "vetting proceeding";
- 5) training in classified information security;
- 6) registering, safe-keeping, processing and making available information obtained in connection with the vetting proceedings conducted, to the extent defined in the personal security questionnaire and industrial security questionnaire;
- 7) organising the supervision of compliance with the classified information security standards;
- 8) protecting classified information in electronic information systems; (and)
- 9) applying physical measures of protecting classified information.

2. The provisions of this Act shall apply to:

- 1) the public authorities, in particular:
 - a) the Sejm and Senate of the Republic of Poland;

- b) the President of the Republic of Poland;
 - c) administrative agencies of the (central) government;
 - d) local government authorities;
 - e) courts and tribunals;
 - f) state inspection and law enforcement authorities;
- 2) the Armed Forces of the Republic of Poland, hereinafter called "the Armed Forces";
 - 3) the National Bank of Poland and state banks;
 - 4) state corporations and state organisations other than those referred to in items 1-3; (and)
 - 5) those businesses and scientific or research-and-development organisations which solicit or perform contracts involving access to classified information, (where the contracts) concern the execution of projects financed wholly or partly with public funds within the meaning of the 10 June 1994 Public Orders Act (...)*.

3. This Act shall be without prejudice to the provisions on the protection of trade secrets or other legally protected secrets laid down in other Acts.

Article 2.

For purposes of this Act:

- 1) state secret--shall mean that classified information defined in the schedule of classified information forming Annex 1 hereto the unauthorised disclosure of which might cause a grave threat to fundamental interests of the Republic of Poland, in particular to independence or inviolability of the territory of the Republic of Poland, national defence interests or security of the state and citizens, or expose those interests to no less than a substantial damage;
- 2) public service secret--shall mean the classified information, other than a state secret, which has been obtained in connection with the discharge of official duties or performance of agency contracts and the unauthorised disclosure of which might damage interests of the state, public interests, or lawfully protected interests of citizens or of an organisation;
- 3) state security services--shall mean the Office for State Security and the Military Information Services;

4) fit and proper to keep secrets--shall mean (one who satisfies) the statutory requirements in respect to protecting classified information against unauthorised disclosure;

5) document--shall mean any classified information recorded on any instrument, in particular in writing, on microfilms, negatives and photographs, on digital recording media and electromagnetic tapes, in the form of a map, sketch, drawing, picture, graphic design, photograph, brochure, book, copy, duplicate, excerpt, abstract from or translation of a document, superfluous or faulty printout, print, film, matrix or optical disc, carbon sheet, carbon tape, likewise electronically recorded classified information;

6) material--shall mean the document, or that object or any part thereof which is subject to protection as classified information, in particular a device, fixture or weapon, whether produced or under development, and a component used for the production thereof;

7) organisation--shall mean any of the bodies referred to in Article 1 clause 2;

8) electronic information system--shall mean a system consisting of equipment, instruments, methods and procedures used by specialised staff in a manner ensuring the generation, storing, processing or transmission of information; (and)

9) electronic information network--shall mean an organisational and technical arrangement whereby certain electronic information systems and connecting facilities and transmission lines are integrated.

Article 3.

Classified information shall be disclosed to none other than those fit and proper to keep secrets and solely to the extent required by the recipient to perform his or her work, discharge official duties, or provide a product under a job contract.

Article 4.

1. The terms of rescinding the obligation of non-disclosure of state and public service secrets in proceedings before courts and other bodies are laid down in separate Acts.

2. Where separate Acts confer upon state agencies, services or institutions or their authorised employees the right to conduct inspections, in particular free access to premises and materials, (and) where the scope of the inspection concerns classified information, such rights shall be exercised subject to the provisions of this Act.

CHAPTER 2 CLASSIFIED INFORMATION PROTECTION COMMITTEE

Article 5.

1. The Council of Ministers' Classified Information Security Committee, hereinafter called "the Committee", is hereby created as an opinion-giving and advisory body on matters of classified information security.

2. The tasks of the Committee shall include specifically:

1) drafting general classified information security guidelines, including organisational and technical standards for protecting classified information against major security threats;

2) giving opinion on directions and plans of action in the face of a special nation-wide threat resulting from the disclosure of classified information being a state secret, in the situation where the application of common constitutional measures will suffice;

3) reviewing and appraising the impact of a special threat situation or of other hazards on the security of classified information and giving opinion on the said subject; 4) drafting government documents designed to ensure the compatibility of the Polish law--to the extent of classified information security--with the commitments arising under international treaties binding on the Republic of Poland;

5) providing opinion on bills and draft programmes, studies, reports and other government documents concerned with protecting classified information, in particular:

a) the classified information security system and its operational foundations in respect to: the arms industry; trading in arms and special equipment; scientific and research-and-development projects serving national defence and state security purposes; preparing the national economy for mobilisation; setting up and managing state reserves; and maintaining the national economy's defence production and repair capacity;

b) the classified information security standards applicable to land use planning and to the development of economic infrastructure, including communications;

6) considering such other matters as the Council of Ministers or the Chairman of the Council of Ministers may refer to the Committee or as may be raised by ministers in connection with the implementation of classified information security tasks.

Article 6.

The Committee shall consist of: the Chairman, Deputy Chairmen, Members and Secretary.

Article 7.

1. The office of Committee Chairman shall be held by the Chairman of the Council of Ministers who shall call Committee meetings and direct the Committee's work.

2. The office of Deputy Chairman shall be held by:

- 1) the minister responsible for internal affairs as the first Deputy Chairman; (and)
- 2) the Minister of Defence as the second Deputy Chairman.

Article 8.

The following officials shall sit on the Committee as Members:

- 1) the ministers responsible for: foreign affairs, the economy, budget, public finance, justice and public administration and the Chief of Staff of the Prime Minister's Chancellery;
- 2) the Secretary of the National Defence Council--Chief of the National Security Office;
- 3) the Chief of the Office for State Security;
- 4) the Chief of the Military Information Services;
- 5) no more than three persons, appointed and recalled by the Chairman of the Council of Ministers, who are capable of contributing importantly to furthering the Committee's tasks due to the experience possessed or office held.

Article 9.

The Committee Secretary shall be appointed and recalled by the Committee Chairman.

Article 10.

The Chairman of the Council of Ministers shall determine by Ordinance:

- 1) the Committee's detailed work procedures;
- 2) the terms of attending Committee meetings; (and)
- 3) the scope of the Committee Secretary's duties.

Article 11.

The following persons may attend Committee meetings with the right to vote:

- 1) a delegated representative of the President of the Republic of Poland;
- 2) the Chairman of the Supreme Board of Inspection;

- 3) the President of the National Bank of Poland;
- 4) duly authorised proxies of the Committee Members referred to in Article 8 items 1-4-- subject to approval of the Committee Chairman;
- 5) a minister other than those referred to in Article 8 item 1--to the extent that the matter coming before the Committee falls within that minister's purview.

Article 12.

The Prime Minister's Chancellery shall ensure support services for the Committee.

Article 13.

1. The Committee Chairman shall annually submit to the Council of Ministers the Committee's work report together with conclusions based on the findings of inspections conducted by state security services regarding compliance with the classified information security provisions.

2. The Committee Chairman shall submit the report referred to in clause 1 to the President of the Republic of Poland and the Chairman of the Sejm Special Services Commission.

CHAPTER 3 PROTECTION OF CLASSIFIED INFORMATION: ORGANISATION OF

Article 14.

1. The state security services shall have the power and authority to:

- 1) examine classified information security (arrangements) and compliance with the respective regulations;
- 2) carry out tasks concerned with the security of electronic information systems and networks;
- 3) conduct vetting proceedings on the terms laid down in this Act;
- 4) protect classified information exchanged between the Republic of Poland and other states and international organisations;
- 5) conduct training and provide advice on matters of classified information security;
(and)
- 6) perform other tasks relating to classified information security, to the extent set out in separate provisions.

2. To the extent essential to the discharge of their functions, the state security services may use information held by the Police, Frontier Guard Service, Military Police, Customs Inspection and Treasury Revenue Inspection authorities and they may, in the process of conducting vetting proceedings, call on the said services and authorities for necessary support.

3. The heads of organisations shall co-operate with the state security services in the course of vetting proceedings, in particular by making available to the state security service civilian or military staff who have presented a written authorisation such information and documents held (by the organisation) as may be necessary for pronouncing the person under review fit and proper to protect secrets.

4. The Chairman of the Council of Ministers shall by Ordinance determine the detailed scope, terms and procedures for:

1) turning over or, respectively, making available to the state security services the information and documents referred to in clause 2; (and)

2) providing the state security services with the support referred to in clause 2.

5. The following shall be specifically set out in the Ordinance referred to in clause 4:

1) the detailed scope, terms and procedure to be observed by the organisation heads when releasing to the state security services information and documents necessary for pronouncing the person under review fit and proper to protect secrets; (and)

2) the scope, terms and procedure to be observed by the Police, Border Guard Service, Military Police, and Customs Inspection and Treasury Revenue Inspection authorities in the process of assisting state security services to the necessary extent in performing actions and tasks involved in vetting proceedings.

Article 15.

In international relations the Chief of the Office for State Security and the Chief of Military Information Services shall perform the function of the national security authorities.

Article 16.

To the extent necessary for inspecting the security of classified information with the status of state secret, civilian and military state security services personnel holding due written authorisations may:

1) freely enter those sites and premises of the inspected organisation where the said information is generated, processed, stored or transmitted;

- 2) examine documents relating to the inspected organisation's state secret security arrangements;
- 3) demand that the electronic information systems and networks used for generating, storing, processing or transmitting the said information be made available for inspection;
- 4) survey such sites and facilities and inspect the progress of such operations as are connected with protecting the said information;
- 5) instruct the heads and personnel of the inspected organisation to submit written and oral explanations and disclose any knowledge relating to espionage or terrorist activities directed against the Republic of Poland or its Armed Forces, or against businesses, scientific or research-and-development organisations--in respect to those products or services of the inspected organisation which have the status of state secret for reasons of national security or national defence and those serving the needs of the Armed Forces;
- 6) seek information, in connection with the inspection in progress, from the organisations other than the one under inspection whose business is connected with the generation, storage, processing, transmission or protection of that classified information which is a state secret, likewise to request explanations from the heads and personnel of those organisations;
- 7) enlist the assistance of experts and specialists--in the event that specialist knowledge is required for establishing certain circumstances disclosed in the course of the inspection; (and)
- 8) attend meetings of executive, managing and supervisory bodies of the inspected organisation, as well as meetings of opinion-giving and advisory bodies for matters of state secret security within the inspected organisation.

Article 17.

1. Article 28, Article 29 item 1, Articles 30-41 and Articles 49-64 of the 23 December 1994 Supreme Board of Inspection Act (...) shall apply respectively to the activities referred to in Article 16 provided that the powers and duties conferred thereby:

- 1) upon the Supreme Board of Inspection--shall be vested in the state security services; (and)
- 2) upon the Supreme Board of Inspection Chairman, Deputy Chairman and staff--shall be vested, respectively, in the Chief, Deputy Chief and authorised officers of the Office for State Security and the Chief, Deputy Chief and authorised military staff of the Military Information Services.

2. The Chairman of the Council of Ministers shall prescribe by Ordinance the detailed security inspection procedure in respect to classified information having the status of a state secret, in particular: the duties of civilian and military state security services personnel supervising and performing the various inspection actions during the course of inspection proceedings; the detailed procedure for preparing the inspection, documenting individual inspection actions, drawing up the record of inspection and post-inspection recommendations and reporting on the findings of an inspection conducted by state security services.

Article 18.

1. The head of the organisation in which classified information is generated, processed, transmitted or stored shall be responsible for the protection thereof.

2. The head of the organisation shall be the direct superior of the executive in charge of protecting classified information, hereinafter called "the security officer", who shall be responsible for ensuring that the organisation complies with the classified information security provisions.

3. A person eligible for the position of security officer in an organisation shall:

- 1) be a Polish citizen;
- 2) have at least a secondary education;
- 3) have been given by the state security services, on the recommendation of the general manager of the organisation, the security clearance referred to in Article 36 clause; (and)
- 4) have undergone training in classified information security.

4. The security officer shall head a specialised service created within the organisation for the protection of classified information, hereinafter called "the security service", whose duties shall include:

- 1) ensuring protection for classified information;
- 2) protecting electronic information systems and networks;
- 3) ensuring physical protection for the organisation;
- 4) inspecting the security of classified information and compliance with the classified information security provisions;
- 5) conducting from time to time inspections of registers, materials and circulation of documents;

6) designing the organisation's security plan and overseeing the implementation thereof;
(and)

7) training employees in classified information protection pursuant to Chapter 8.

5. A person eligible for employment in the security service of an organisation shall:

1) be a Polish citizen;

2) have been given the security clearance referred to in Article 36 clause 2; (and)

3) have undergone training in classified information security

6. Should an extraordinary state be imposed, the security officer may request immediate support from other services of the organisation--to the extent necessary for discharging the responsibilities of the office.

7. To the extent of the responsibilities of the office, the security officer shall co-operate with appropriate units and organisations of the state security services. The security officer shall keep the head of the organisation informed on a day-to-day basis of the progress of that co-operation.

8. The security officer shall design a contingency plan for handling the materials containing classified information with the status of a state secret in the event that an extraordinary state should be imposed.

9. The security officer shall take steps to clarify the circumstances of any case of non-compliance with the classified information security provisions and he or she shall duly notify the head of the organisation and--in the event of non-compliance with regulations on protecting classified information rated "confidential" or above--the appropriate state security service.

CHAPTER 4. CLASSIFIED INFORMATION: SECRECY RATINGS

Article 19.

1. The rating of classified information shall mean according to that information, explicitly and in a manner provided in this Act, one of the levels of secrecy referred to in Article 23 and Article 24.

2. The rating of classified information embodied in a certain material, in particular of that recorded in a document, shall be executed by means of marking that material with an appropriate secrecy specification.

3. Classified information (and) materials, in particular documents or collections of documents, shall be accorded a secrecy classification equal to or higher than that given to the highest-rated information or, as applicable, the highest-rated document in the collection of documents.

4. Different parts (chapters, enclosures, annexes) of a document or different documents in a collection of documents may be accorded different secrecy classifications, providing that their secrecy rating shall be explicitly marked and providing that when a document or part thereof is detached from the whole, its classification shall be explicitly indicated.

Article 20.

1. Subject to clause 2, information accorded a certain secrecy classification shall be subject to protection according to the provisions of this Act which concern classified information bearing that secrecy classification. This shall be construed in particular to mean that such information:

1) shall be disclosed to no other person than those authorised to obtain access to classified information with a given secrecy classification;

2) shall be generated, processed, transmitted or stored in conditions preventing its unauthorised disclosure, according to the statutory standards on the secret records office, circulation (of classified information), and physical protective measures commensurate with that secrecy classification; (and)

3) shall be accorded the degree of protection appropriate for that secrecy classification, using the measures described in Chapter 9.

2. The security officer shall design and the general manager shall approve the organisation's detailed in-house security standards in respect to classified information marked "restricted".

Article 21.

1. Information shall be accorded a certain secrecy classification by the person authorised to sign a given document or to rate for secrecy a given non-document material.

2. The power to give, reduce and cancel the secrecy classification shall be exercised solely within the scope of the person's right of access to classified information.

3. The person referred to in clause 1 shall bear the responsibility for giving secrecy classification and the classification shall not be reduced or removed without the consent of that person or his or her superior. This shall apply equally to the person who has supplied data for a collective document.

4. Increasing or reducing a given secrecy classification shall be inadmissible.

5. In the event that a certain material has been given an evidently overrated or underrated secrecy classification, the recipient of the same shall notify the person referred to in clause 1 or that person's superior. Where the person or the person's superior resolves to modify the material's secrecy classification, he or she shall advise the recipients to that effect. The recipients who have transferred the material to next recipients are responsible for informing them of the modified secrecy classification.

Article 22.

The organisation heads shall arrange for their employees to be trained in ranking classified information, in giving appropriate secrecy classifications in the secrecy classification modification and removal procedures.

Article 23.

1. The classified information accorded the status of a state secret shall be rated as:

1) "top secret"--where an unauthorised disclosure thereof might cause a grave threat to the independence of the Republic of Poland (or to) the inviolability of its territory or its international relations, or carry a threat of irreversible or heavy injuries to national defence interests, to the security of the state and citizens or to other important state interests, or expose those interests to great danger; (and)

2) "secret"--where an unauthorised disclosure thereof might cause a threat to the international position of the state, to national defence interests, security interests of the state and citizens, or other important interests of the state, or expose those interests to a substantial damage.

2. The classified information accorded the status of a public service secret shall be rated as:

1) "confidential"--where an unauthorised disclosure thereof would damage interests of the state, public interests or certain legally protected interests of citizens; (and)

2) "restricted"--where an unauthorised disclosure thereof might damage certain legally protected interests of citizens or of the organisation.

3. The minister responsible for internal affairs and the Minister of Defence shall prescribe by Order, upon inviting the opinion of the Office for State Security Chief, the manner of classifying materials, including according to their secrecy level, and the manner of marking the material's secrecy classification.

4. The minister responsible for internal affairs and the Minister of Defence may prescribe by Order, upon inviting the opinion of the Office for State Security Chief, certain additional marks to be put on materials containing classified information before those referred to in clause 1 and clause 2, as instructions on a special manner of handling those materials, (or) a special manner of generating, processing, transferring or storing the materials so marked and the circle of authorised recipients thereof-- when warranted by increased classified information security requirements, including those arising under international agreements to which the Republic of Poland is a party.

Article 24.

The materials received from abroad or dispatched abroad for the purpose of implementing ratified international agreements shall be marked with the secrecy classification, as provided in this Act, which is appropriate to their contents and with a foreign counterpart of that secrecy classification.

Article 25.

1. Subject to clause 2, classified information with the status of a state secret shall be subject to protection pursuant to this Act for a period of 50 years from being generated.

2. The following information shall be subject to protection regardless of the elapse of time:

1) data identifying the civilian and military state security services staff engaged in operational-surveillance tasks;

2) data identifying those who assisted the state bodies, services and institutions authorised under this Act to carry out operational-surveillance tasks in the execution thereof; (and)

3) that classified information obtained from other states or international organisations which has been supplied subject to that condition.

2. Classified information with the status of a public service secret shall be subject to protection pursuant to this Act for a period of:

1) 5 years--in respect to information classified "confidential"; (and)

2) 2 years--in respect to information classified "restricted"

--unless the person referred to in Article 21 clause 1 has set a shorter (protection) period.

4. Subject to clause 2, the Council of Ministers may identify by Ordinance that information classified "secret" which is no longer a state secret, provided no less than 20 years have elapsed from the date of generation thereof.

4. In the event of an organisational change, be it a dissolution, abolition, liquidation, transformation or re-organisation, affecting the position or function of the person referred to in Article 21 clause 1, the said person's powers of giving, reducing or removing secrecy classification of material and setting a period during which classified information is subject to protection shall transfer to his or her legal successor. In the absence of a legal successor, those powers shall transfer to the appropriate the state security service.

CHAPTER 5 ACCESS TO CLASSIFIED INFORMATION: VETTING PROCEEDINGS

Article 26.

1. Subject to clause 2, the organisation head shall separately determine for each secrecy classification the positions or kinds of out-contracted jobs which may involve access to classified information.
2. The Council of Ministers shall determine by Ordinance the positions in administrative bodies of the government and the kinds of jobs out-contracted by administrative bodies of the government which may involve access to classified information having the status of a state secret.

Article 27.

1. Subject to clause 2, clause 3 and clauses 6-8, a person shall be admitted to employment or service in the position referred to in Article 26 or to performing the job referred to in Article 26 after:

- 1) vetting proceedings have been conducted in respect to him or her; (and)
- 2) he or she has undergone training in classified information security.

2. No vetting proceedings shall be conducted in respect to persons holding the following functions: the President of the Republic of Poland, Sejm Speaker and Senate Speaker.

3. Subject to clause 4, no vetting proceedings shall be conducted in respect to the Sejm Deputies and Senators.

4. The Sejm Speaker or the Senate Speaker shall request the state security services to conduct vetting proceedings in respect to those Sejm Deputies or Senators whose official duties require access to information classified as "top secret", subject to the investigated person's consent.

5. When the person referred to in clause 4 has been refused a security clearance, the Chairman of the Council of Ministers shall, subject to consent of the said person, advise

the Sejm Speaker(when the refusal concerns a Sejm Deputy(or the Senate Speaker(when the refusal concerns a Senator(of the reasons for the refusal.

6. No vetting proceedings shall be conducted in respect to persons holding the following positions: Chairman of the Council of Ministers, member of the Council of Ministers, President of the Supreme Court, President of the Supreme Administrative Court, Chairman of the Constitutional Tribunal, President of the National Bank of Poland, Chairman of the Supreme Board of Inspection, Ombudsman, General Inspector for Personal Data Protection, Public Interest Advocate, members of the Monetary Policy Council, members of the National Broadcasting Board and the Chiefs of Staff of the Chancellery of the President of the Republic of Poland, Chancellery of the Sejm, Chancellery of the Senate and Prime Minister's Chancellery.

7. The state security services shall conduct vetting proceedings in respect to candidates to the positions referred to in clause 6 on a motion of the body authorised to fill the said positions by appointment. When the Sejm or the Senate is the authorised appointing body, the motion shall be made, respectively, by the Sejm Speaker or Senate Speaker. At the conclusion of the proceedings, the appropriate security service shall furnish the President of the Republic of Poland, Sejm Speaker or Senate Speaker with its duly substantiated opinion.

8. When a state of emergency has been imposed and is in effect, the President of the Republic of Poland or the Chairman of the Council of Ministers may, within their respective areas of responsibility, waive the vetting proceedings in respect to the person referred to in clause 1 unless there are grounds to consider that person unfit to keep secrets.

9. The President of the Republic of Poland and the Sejm and Senate Speakers shall acquaint themselves with the provisions on protecting classified information and they shall furnish declarations to the effect that they are familiar with those provisions. The Sejm Deputies, Senators and the persons referred to in clause 6 shall furnish such declarations upon undergoing training in classified information security.

Article 28.

1. Subject to clause 2, the following persons shall not be admitted to employment or service in a position involving access to classified information or to the performance of a job involving access to classified information:

1) those who are not Polish citizens, subject to Article 67 clause 4;

2) those sentenced under valid verdicts for a deliberate offence subject to public prosecution, including such an offence committed outside the territory of the Republic of Poland; or

3) those not holding a security clearance, except for the persons referred to in Article 27 clause 2, clause 3, clause 6 and clause 8.

2. When international treaties ratified by the Republic of Poland require, subject to reciprocity, that foreign citizens charged with performing certain tasks for a foreign state or an international organisation on the territory of the Republic of Poland be given access to classified information, no vetting proceedings shall be conducted (in respect to those foreign citizens).

Article 29.

The vetting proceedings referred to in Article 39 shall be conducted upon a written motion of the person who is authorised under separate provisions to fill certain positions by appointment or to out-contract certain jobs, hereinafter called the "authorised appointing official", by:

1) the Military Information Services (when the appointment or contract sought concerns the defence potential of the state:

a) in respect to the Armed Services' military personnel on active service and civilian personnel, except for (the personnel of) military units reporting to the minister responsible for internal affairs;

b) in businesses, in scientific and research-and-development organisations established by the Minister of Defence as the parent body, and in other organisations (to the extent of those entities' involvement in the production of goods or provision of services which are state secrets for reasons of their importance to the national defence potential and the Armed Forces' needs;

c) in businesses which trade in products, processes and licences which are state secrets for reasons of national defence potential, when the Armed Forces or organisations reporting to the Minister of Defence are parties to that trade; (and)

d) in military law enforcement and order-keeping organisations;

2) the Office for State Security (when the person seeks an appointment, employment, or contract in circumstances other than those referred to in clause 1.

Article 30.

The Office for State Security, Military Information Services, Police, Frontier Guard Service and Penitentiary Service shall, in exercise of their powers, conduct vetting proceedings in respect to those seeking service or employment, pursuant to the respective provisions of this Act. The aforesaid shall apply equally to those in the service or employment of the above mentioned bodies and services.

Article 31.

1. The vetting proceedings shall not be conducted otherwise than subject to the written consent of the person concerned, hereinafter called the "investigated person".
2. An application of the person referred to in Article 29 for employment or service in any position, which under the provisions of this Act is subject to a prior vetting proceeding, shall not be considered in the absence of the investigated person's consent to submit to the vetting proceedings.
3. The vetting proceedings may be waived in the event that the person referred to in clause 1 has presented an appropriate security clearance.

Article 32.

The collecting and processing of information about third parties identified in the personal security questionnaire referred to in Article 37 clause 2 item 1 without the knowledge and consent of those third parties is hereby permitted to the extent necessary for establishing whether the investigated person is fit and proper to protect secrets.

Article 33.

The holder of a security clearance which gives him or her access to information with a higher secrecy classification shall (by force of being given such a security clearance) have access to information with a lower secrecy classification solely to the extent defined in Article 3.

Article 34.

In the process of conducting the vetting proceedings the state security services and the security officer shall be guided by the principles of fairness and impartiality and they shall exercise the highest degree of care to ensure that the proceedings conform to the provisions of this Act.

Article 35.

1. The vetting proceedings shall be conducted with a view to establishing whether or not the investigated person is fit and proper to protect secrets.
2. In the course of the vetting proceedings it shall be established whether or not doubts exist as to:
 - 1) the investigated person having been (at any time) involved, whether as a member, accomplice or supporter, in espionage, terrorist, or subversive activities or other activities directed against the Republic of Poland;

2) the investigated person having concealed or deliberately misrepresented in the course of the vetting proceedings information pertinent to the security of classified information, likewise as to the existence of any circumstances having a bearing on the investigated person and capable of rendering him or her vulnerable to blackmail or pressure;

3) the investigated person having abided by the constitutional order of the Republic of Poland, in particular as to his or her having (at any time) belonged to or co-operated with the political parties or other organisations referred to in Article 13 of the Constitution; (and)

4) the investigated person being exposed to foreign special services' attempts at recruiting or establishing contact, in particular as to whether pressure might be exerted on him or her to that end.

3. In the course of the vetting proceedings referred to in Article 36 clause 1 item 2 and item 3 it shall be additionally established whether or not the (investigated person's trustworthiness) is open to doubt:

1) due to a noticeable disparity of his or her living standard and income;

2) when information has been received to the effect that the investigated person suffers from a mental disease or other kind of mental disorder which limits his or her mental competence and is capable of affecting his or her ability to discharge the duties of an office or perform a job which involves access to classified information being a state secret; (and)

3) for reasons relating to an addiction to alcohol or drugs.

4. The state security service may, with the aim of ascertaining the answers referred to in clause 3 item 2 and item 3, direct the investigated person to submit to specialised tests and to produce the results thereof.

Article 36.

1. The following (kinds of) vetting proceedings shall be conducted depending on the position or out-contracted job sought by a given person:

1) standard when the position or contract involves access to classified information which is a public service secret;

2) extended when the position or contract involves access to information classified "secret"; (and)

3) special when the position or contract involves access to information classified "top secret". 2. At the conclusion of the vetting proceedings, a security clearance shall be issued or refused.

3. The minister responsible for internal affairs shall prescribe by Order the specimens of:

- 1) the security clearance; (or)
- 2) the refusal to issue a security clearance.

4. The following shall be stated at all times in the security clearance or, as the case may be, in the refusal to issue a security clearance:

- 1) the legal basis;
- 2) the person requesting the institution of vetting proceedings;
- 3) the state security service or the security officer conducting the vetting proceedings;
- 4) the date and place of issue;
- 5) the name (given and surname) and the date of birth of the investigated person;
- 6) the kind of vetting proceedings conducted, indicating the security classification of information to which the investigated person may thereby obtain access;
- 7) a statement that a security clearance has been given or, as the case may be, refused;
- 8) the validity date; (and)
- 9) the seal with the name and a legible signature of the authorised civilian or military state security service official or security officer.

Article 37.

1. The standard vetting proceedings shall be conducted by the security officer on the written instructions of the organisation head.

2. The standard vetting proceedings shall cover:

- 1) filling a personal security questionnaire, hereinafter called the "questionnaire"; the questionnaire and instructions on filling the same constitute Annex 2 to this Act;
- 2) cross-checking, to the necessary extent, the answers given in the questionnaire against records, registers and files, in particular against the Central Register of Sentenced Persons and the Register of Sentenced and Detained Persons;

3) cross-checking the answers given in the questionnaire against non-public records and registers; this shall be done by the appropriate state security service upon a written motion by the security officer, solely in respect to candidates for positions involving access to information classified "confidential"; (and)

4) verifying the investigated person's marital status.

3. The investigated person shall personally fill and sign the questionnaire.

4. False or incomplete information deliberately supplied in the questionnaire shall constitute a basis for the security officer to refuse the security clearance.

5. In the course of the cross-checking referred to in clause 2 item 3, the state security services may interview the investigated person in order to clarify unclear or contradictory points in the information collected.

6. The state security services shall notify the security officer in writing of the results of the action referred to in clause 5.

7. After the standard vetting proceedings have been completed with a positive result, the security officer shall issue the security clearance, furnish the same to the investigated person and notify the authorised appointing official to that effect.

8. The security officer shall refuse to issue the security clearance unless the doubts referred to in Article 35 clause 2 have been removed.

9. The security officer may refuse to give a security clearance in the event that vetting proceedings required to authorise (the investigated person's) access to information classified "confidential" could not be conducted successfully for reasons beyond the security officer's control.

10. The security officer shall notify the authorised appointment official in writing of having refused to issue the security clearance.

Article 38.

1. The extended vetting proceedings shall be conducted by the appropriate state security service on a written motion of the authorised appointing official. Those proceedings shall include:

1) the steps referred to in Article 37 clauses 2-5;

2) an inquiry conducted at the investigated person's place of residence, when this is necessary for corroborating the particulars stated in the questionnaire;

3) interviews with superiors of the investigated person and with other persons, when information obtained regarding the investigated person so warrants;

4) in justified cases, checking the balance in (the investigated person's) bank account and transactions made from that account, pursuant to Article 104 clause 2 of the 29 August 1997 Banking Law Act (...) * and the investigated person's debts, in particular his or her outstanding liabilities to the Treasury (when this should be necessary for corroborating the particulars stated in the questionnaire; Article 82 paragraph 1 and paragraph 2 and Article 182 of the 29 August 1997 Tax Law Act (...) * and Article 33 clause 1 of the 28 September 1991 Treasury Revenue Inspection Act (...) * shall apply, respectively.

2. The inquiry referred to in clause 1 item 2 shall be conducted by the state security services according to the respective provisions of the Code of Criminal Procedures and the regulations on inquiry in domicile issued pursuant to the Code of Criminal Procedures.

Article 39.

The special vetting proceedings shall be conducted by the appropriate state security service on a written motion of the authorised appointing official. Those proceedings shall cover the steps referred to in Article 38 and, additionally:

1) an interview with the investigated person; (and)

2) an interview conducted by the state security services with three persons named by the investigated person, with the object of confirming the investigated person's identity.

Article 40.

1. Should such doubts arise in the course of extended or special vetting proceedings which render a determination impossible as to whether or not the investigated person is fit and proper to protect secrets, the (appropriate) state security service shall give the investigated person the opportunity of stating personally his or her position on the actual premises underlying those doubts. The investigated person shall be heard in a manner ensuring the protection of his or her personal data according to Article 12 clause 1 of the 6 April 1990 Office for State Security Act (...) * hereinafter called the "Office for State Security Act". The investigated person may come for the hearing accompanied by his or her legal representative.

2. The state security services shall waive the action referred to in clause 1 in the event that the principle of protecting classified information with the status of a state secret might be infringed by the conduct thereof.

3. Article 37 clauses 7-10 shall apply, respectively, to extended vetting proceedings and special vetting proceedings.

Article 41.

1. The refusal to give a security clearance shall not be binding on the authorised appointing official responsible for filling the position which involves access to classified information with the status of a public service secret.

2. In the event that a position or job contract is given to a person who has been refused a security clearance in respect to information classified as "confidential" or when (such a person) is given access to information classified as a state secret, the authorised appointing official shall forthwith notify the appropriate state security service to that effect.

3. Vetting proceedings in respect to the person who has been refused a security clearance shall be conducted no earlier than 1 year from the date on which he or she was refused the security clearance.

Article 42.

The provisions of the Code of Administrative Proceedings and the provisions on appeal by complaint to the Supreme Administrative Court shall not apply to vetting proceedings.

2. All actions performed by a security officer and the state security services during the course of vetting proceedings shall be documented in a reliable manner and shall be completed before the elapse of:

1) 1 month from the date of the written order to conduct standard vetting proceeding;

2) 2 months--from the date of submission of the motion for extended vetting proceedings and the filled questionnaire; (and) 3) 3 months from the date of submission of the motion for special vetting proceedings and the filled questionnaire.

3. The files of completed vetting proceedings on persons seeking positions or contracts involving access to classified information with the status of a public service secret shall be kept by the security officer and made available for inspection solely:

1) to the investigated person seeking the position in question;

2) at the request of the court or public prosecutor, for purposes of a criminal prosecution; (and)

3) to the authorised appointing official or the appropriate state security services for purposes of vetting proceedings.

4. The files of completed vetting proceedings on persons seeking positions or contracts involving access to information classified as a state secret shall be kept as separate parts of the state security services' archives.

5. The state security services shall, to the extent of their respective duties, keep registers of the persons given a security clearance and those holding the positions and performing the jobs which involve access to information classified "confidential" or which are state secrets. The register entries and the files of vetting proceedings shall be made available for inspection solely at the request of the court or public prosecutor for purposes of a criminal prosecution, or to the state security services for purposes of vetting proceedings.

6. The register entries referred to in clause 5 shall cover solely:

1) regarding the person(his or her given name and surname, father's name, date and place of birth, registered address or place of abode, name and address of the employer organisation, name of the unit in which the person is employed within the organisation and position held and the code of the vetting proceedings file; (and)

2) regarding the position held or out-contracted job performed(the date on which the position was assumed or the performance of the job commenced, the kinds of classified information accessible to the holder of that position by virtue of the office and the issuing date and number of the security clearance.

7. The Chairman of the Council of Ministers shall prescribe by Ordinance the manner and procedure for giving access to the data referred to in clause 5.

Article 43.

1. The authorised appointing official may, within 1 month from being notified of the state security services' refusal to issue a security clearance, apply to the Council of Ministers ex officio, subject to the consent of the investigated person or at his or her request, for review vetting proceedings.

2. The appropriate state security service shall turn over to the Chairman of the Council of Ministers forthwith, and no later than 7 days from receiving the Chairman of the Council of Ministers' instructions to that effect, the materials relating to the vetting proceedings for the purpose of conducting the review vetting proceedings.

3. Should the Chairman of the Council of Ministers establish that the investigated person is fit and proper to protect secrets, he or she shall give an adjudication, which shall be binding on the appropriate state security service, ordering that the security clearance be issued or the vetting proceedings supplemented. In the event that the review vetting proceedings have confirmed the findings of the state security service, the Chairman of the Council of Ministers shall notify the body authorised to fill the position in question to that effect.

4. On completing the review vetting proceedings the Chairman of the Council of Ministers shall forthwith return to the appropriate state security service the materials referred to in clause 2.

Article 44.

1. The vetting proceedings shall be repeated at the following intervals in respect to the persons who hold the positions or perform the out-contracted jobs involving access to information classified:

1) "confidential"(every 10 years;

2) "secret"(every 5 years; (and)

3) "top secret"(every 3 years

--from the security clearance issuing date.

2. The motion for instituting consecutive vetting proceedings shall be filed at least 6 months before the expiration of the security clearance.

Article 45.

1. When new facts concerning the investigated person are revealed and when those facts suggest that he or she is not fit and proper to protect secrets, the state security services or the security officer shall conduct consecutive vetting proceedings regardless of the intervals referred to in Article 44 clause 1.

2. The state security services shall notify the authorised appointing official and the investigated person of the institution of the consecutive vetting proceedings referred to in clause 1.

Article 46.

Subject to Article 47, the provisions on the vetting proceedings proper shall apply to the consecutive proceedings.

Article 47.

On receiving the notification referred to in Article 45 clause 2, the organisation head may restrict or exclude access to classified information by the person subject to the consecutive vetting proceedings.

Article 48.

The security officer shall keep an index of the positions and out-contracted jobs (involving access to classified information) and of the persons admitted to employment or service in the positions involving access to classified information. Article 42 clause 5 and

clause 6 and the regulations issued pursuant to Article 42 clause 7 shall apply, respectively.

CHAPTER 6 PROVIDING ACCESS TO CLASSIFIED INFORMATION

Article 49.

1. When exceptional circumstances so warrant, certain persons or institutions may be given access to classified information with the status of a state secret under a written authorisation given by the Chief of Staff of, respectively: the Chancellery of the President of the Republic of Poland, the Sejm Chancellery, the Senate Chancellery and the Chancellery of the Prime Minister, or by the minister responsible for a given administrative branch of the government or the head of a central office (and, in the absence of those, under a written authorisation issued by the appropriate state security service).

2. The organisation head may issue a written authorisation for (a person's or institution's) access to classified information with the status of a public service secret exclusively in respect to information generated within the organisation.

3. The authorisation of access to classified information shall not be construed as a modification or removal of the security classification of that information; the authorisation shall at all times specify the extent of access in terms of those to whom the classified information may be made available and the scope of information made available.

CHAPTER 7 SECRET RECORDS OFFICE: SUPERVISING THE CIRCULATION OF DOCUMENTS

Article 50.

1. The organisation in which documents containing information which is classified "confidential" or which is a state secret are generated, processed, transmitted or stored shall organise a records office hereinafter called the "secret records office".

2. The secret records office shall be a separate entity reporting directly to the security officer and it shall be responsible for proper registration, storage and circulation of such documents and for releasing the same to duly authorised persons. The secret records office shall be set up on separate premises which shall be secured according to the provisions on physical means for protecting classified information and it shall be run by members of the (organisation's) security service personnel.

Article 51.

Separate secret records offices shall be set up for documents with different secrecy classifications. The above notwithstanding, a single secret records office may be

established providing that the documents with different secrecy classifications shall be physically separated and dealt with by a person holding the security clearance commensurate with the highest secrecy classification accorded to the documents generated, processed, transmitted or stored in that secret records office.

Article 52.

1. The secret records office shall be organised in a manner ensuring that the whereabouts of any classified document held by the organisation are capable of being identified under any circumstances.
2. The documents classified "top secret" and "secret" shall not be released for removal from the secret records office otherwise than to the recipients who are capable of ensuring the protection of such documents against any unauthorised disclosure. When (the recipient's ability to ensure) those security standards are in doubt, the document concerned shall be made available on the premises only.
3. The secret records office shall refuse to make available or release the document referred to in Article 50 clause 1 to persons lacking the appropriate security clearance.
4. The fact that the authorised person has familiarised himself or herself with a document containing information classified as a state secret shall be noted on the document's reader card.

Article 53.

1. The Council of Ministers shall prescribe by Ordinance:
 - 1) the requirements concerning the organisation of the secret records office;
 - 2) the extent and conditions for administering physical protective measures;
 - 3) the procedure for the circulation of classified information; (and)
 - 4) the reader card specimen.
2. The Minister of Defence; ministers responsible for internal affairs, public administration, foreign affairs, public finance, budget and financial institutions; the President of the National Bank of Poland; Chairman of the Supreme Board of Inspection; Chiefs of Staff of the Chancellery of the President of the Republic of Poland, the Sejm Chancellery, the Senate Chancellery, the Prime Minister's Chancellery; and Chief of the Office for State Security shall prescribe, within their respective areas of responsibility, the special standards on the organisation of secret records offices, application of physical protective measures and circulation of classified information.

3. The minister responsible for internal affairs and the Minister of Defence shall determine by Order, upon inviting the opinion of the Chief of the Office for State Security, the procedure and manner of:

- 1) receiving;
- 2) transporting;
- 3) releasing; (and)
- 4) protecting materials

(to protect the same against an unauthorised disclosure, loss, damage or destruction.

CHAPTER 8 TRAINING IN CLASSIFIED INFORMATION SECURITY

Article 54.

1. Before a person is admitted to work or render service which involves access to classified information, he or she shall undergo training in classified information security which shall be conducted with the aim of making the person aware of:

- 1) threats from foreign special services acting against the Republic of Poland and its allied states and threats from terrorist organisations;
- 2) the provisions on protecting classified information and the liability for disclosure thereof;
- 3) the standards and requirements for protecting classified information to the extent necessary for performing the work or rendering services;
- 4) the manner of protecting information classified as a state secret and the actions to be taken when that information is at risk or has been disclosed; (and)
- 5) criminal, disciplinary and service liability for violating the provisions on protecting classified information.

2. The training referred to in clause 1 shall be conducted by:

- 1) civilian and military personnel of the state security services (in respect to the persons referred to in Article 27 clauses 3-8 and in respect to security officers; (and)
- 2) security officers (in respect to those employed or serving in organisations (which receive classified information).

3. The costs of training shall be met by the organisation in which the trainee is employed or serves.

4. The respective rights and commitments of the one who organises and the one who attends the training referred to in clause 2 item 1 shall be determined in a contract entered into by those parties.

Article 55.

The minister responsible for internal affairs shall prescribe by Order the specimen of a training certificate, including a separate certificate for those trained by the state security services.

CHAPTER 9 PHYSICAL MEASURES FOR PROTECTING CLASSIFIED INFORMATION

Article 56.

1. The organisations in which materials containing classified information are generated, processed, transmitted or stored shall apply physical protective measures to prevent unauthorised access thereto, in particular to protect (such materials) against:

- 1) activities by foreign special services;
- 2) terrorist assault or sabotage;
- 3) theft or destruction;
- 4) attempted entry by unauthorised persons; (and)
- 5) unauthorised access by employees to materials with a higher security classification.

2. The physical protective measures shall be applied in such a scope as is commensurate with the security classification and amount of classified information, the number of those employees or personnel (in the organisation) who have access to that information and their level of access and it shall duly take into account the state security services' instructions, in particular on precautions against threats emanating from foreign special services, including (threats to) an allied state.

Article 57.

The following steps shall be taken with the aim of preventing any unauthorised access to classified information:

- 1) certain premises and facilities, hereinafter called "security zones", shall be isolated and the entry, exit and presence thereon shall be subjected to special supervision;

- 2) administrative zones for the inspection of persons and vehicles shall be established around the security zones;
- 3) a system of passes or another system for authorising the entry into, presence in and exit from the security zone and for keeping the keys to the protected premises, safes and other receptacles for information classified as a state secret shall be established;
- 4) arrangements shall be made for training security service staff pursuant to this Act to guard the security zones and administrative zones; (and)
- 5) the equipment and devices used to protect classified information shall have qualification certificates issued pursuant to separate provisions.

Article 58.

1. When circumstances so warrant, special security zones shall be constantly guarded and the use of physical measures for the protection of classified information shall be established to protect information which is a state secret, in particular conversations and meetings concerning that information.
2. The premises within the special security zone shall be arranged and furnished in such a manner that devices preventing sound and visual monitoring of those premises can be installed thereon.
3. Bringing unauthorised materials and devices into or removing such items from a special security zone prior to its inspection by authorised security service personnel is hereby forbidden.

Article 59.

The security officers shall oversee on a day-to-day basis the administration of physical protective measures.

CHAPTER 10 SECURITY OF ELECTRONIC INFORMATION SYSTEMS AND NETWORKS

Article 60.

1. The electronic information systems and networks which serve generate, process or transmit information classified as a state secret shall be subject to special protection against any unauthorised disclosure and against the likelihood of accidental or deliberate exposure.
2. The classified information which is a state secret may be transmitted through electronic information systems and networks consisting of certified cryptographic equipment and

devices provided that only those cryptographic methods and protective measures which are admitted for use under special security standards are applied in the process, pursuant to Article 61 and Article 62.

3. The special security standards for electronic information systems and networks shall consist of the complete and comprehensive description of their construction, operating principles and operating methods, inclusive of the security procedures to be observed during the designing, putting on line and operating of the system or network concerned. The security procedures shall cover the terms and manner of proceedings on matters relating to classified information security, likewise the extent of the liability of the electronic information network or system users and of the employees who have access to the system or network concerned.

4. The Council of Ministers shall prescribe by Ordinance the basic electronic information security requirements to be satisfied by the electronic information systems and networks in which or with the aid of which classified information is generated, processed, stored or transmitted and the guidelines for designing detailed security standards for those systems and networks.

5. The Ordinance referred to in clause 4 shall specifically set out the basic electronic information system and network security specifications in respect to physical, electromagnetic and cryptographic protection and secure transmission through the electronic information systems or networks in which or with the aid of which classified information is generated, processed, stored or transmitted.

Article 61.

1. The head of the organisation shall design special security standards and submit the same to the state security services and he or she shall be responsible for the operation and security of the electronic information network or system.

2. The special security standards covering such cryptographic, electromagnetic, technical and organisational protective measures as may be appropriate for the electronic information system and network in which classified information being a state secret is to be generated, processed, stored or transmitted shall be approved on a case-by-case basis by the state security services within 30 days of being submitted.

3. The special security standards for the electronic information systems and networks in which information classified as a public service secret is to be generated, processed, stored or transmitted shall be submitted to the state security services. Failing an objection by the state security services within 30 days from the submission of the special security standards, the electronic information network or system may be put on line.

Article 62.

1. For information which is a state secret to be generated, stored, processed or transmitted according to the appropriate security classification, a system certificate issued by the appropriate state security service shall be required.

2. The certificate referred to in clause 1 shall be issued on the basis of:

1) an inspection and assessment of the electronic information system's or network's capacity for protecting classified information against any unauthorised disclosure and against the likelihood of exposure;

2) (the results of) vetting proceedings conducted pursuant to this Act; (and)

3) the special system security standards or electronic information network security standards approved by the state security services.

Article 63.

1. The head of the organisation shall appoint:

1) the person or task force, hereinafter called the "system administrator", responsible for the running of the electronic information system or network and for ensuring compliance with the principles and standards of electronic information system and network security; (and)

2) the member of the security service responsible for monitoring on a day-to-day basis the compatibility of the operations of the electronic information system or network with the special security standards referred to in Article 61 clause 2 and clause 3.

2. The state security services shall give the head of the organisations referred to in Article 61 clause 1 such support as may be necessary for the discharge of their tasks.

Article 64.

The person eligible for the position as the system administrator or for the function assigned to the security service staff member referred to in Article 63 clause 1 item 2 shall satisfy such criteria set out in Article 18 clause 5 as are appropriate to the security classification of the information generated, stored, processed or transmitted in the systems or networks concerned and shall have undergone specialised training conducted by the state security services.

CHAPTER 11 INDUSTRIAL SECURITY

Article 65.

1. The (owner of) the business or, as applicable, the scientific or research-and-development organisation soliciting or performing that contract referred to in Article 1

clause 2 item 5, hereinafter called the "contract", the performance of which involves access to information classified as a state secret shall protect the said information.

2. The contract shall at all times state:

1) the detailed requirements in respect to protecting such information classified as a state secret as may be disclosed to the business or, as the case may be, scientific or research-and-development organisation in connection with the performance of the contract, hereinafter called "industrial security instructions". The industrial security instructions shall in each case be commensurate with the amount and security classification of the information (to be disclosed) and with the number of persons having access thereto;

2) the consequences and scope of the parties' liability for non-performance or faulty performance of the obligations arising under this Act and for non-compliance with the requirements laid down in the industrial security instructions.

3. The contract may also determine requirements concerning the protection of information classified as a public service secret. Clause 2 shall apply respectively.

Article 66.

An organisation entering into the contract shall appoint one person to be responsible for overseeing, inspecting, training and counselling (to the extent of the discharge by the business or, as the case may be, the scientific or research-and-development organisation, of the obligation to protect any classified information disclosed to them.

Article 67.

1. The state security services shall (each within its respective area of responsibility) conduct vetting proceedings in the business or, as the case may be, the scientific or research-and-development organisation referred to in Article 65 clause 1.

2. The following persons shall be subject to the vetting proceedings:

f1) those in the positions concerned with the management (or) performance of the contract or with the direct implementation thereof in the business or the scientific or research-and-development organisation;

2) those who, acting on behalf of the person referred to in item 1, take part in transactions preparatory to the execution of the contract, when such actions involve access to classified information;

3) the security service personnel; (and)

4) that business acting for the person referred to in item 1 which has been licensed to render, on a commercial basis, personal and property protection services.

3. The following shall likewise be investigated:

- 1) the structure and origin of the capital of the business;
- 2) the organisational structure of the business or, as the case may be, of the scientific or research-and-development organisation and its governing bodies; (and)
- 3) the financial position and sources of the financial assets held by the entities referred to in clause 2.

4. The requirement laid down in Article 28 clause 1 item 1 shall not apply to the persons referred to in clause 2 items 1-3.

Article 68.

1. The investigation referred to in Article 67 clause 3 shall be conducted on the basis of the information stated in the industrial security questionnaire filed by the business, scientific organisation or research-and-development organisation.

2. The industrial security questionnaire shall contain in particular:

- 1) data concerning the (respondent's) legal status;
- 2) data concerning the (respondent's) organisational and capital structure;
- 3) data concerning the (respondent's) governing bodies or managing bodies;
- 4) an index of the employees authorised to have access to classified information;
- 5) an index of the employees who should be given access to classified information in connection with proceedings conducive to the execution or performance of the contract;
- 6) data on the system for protecting persons, materials and facilities maintained by the business or, as the case may be, the scientific or research-and-development organisation;
- 7) an index of the persons to be made responsible, on behalf of the business, scientific organisation or research-and-development organisation, for the security of classified information released to that business, scientific or research-and-development organisation; (and)
- 8) a legible signature of the person authorised to make statements of will for the business or for the head of the scientific organisation or research-and-development organisation.

3. The business or, as applicable, the scientific organisation or research-and-development organisation shall forthwith inform the state security services and the persons referred to

in Article 66 of any changes which have a bearing on the particulars given in the industrial security questionnaire.

Article 69.

In the event that the proceedings referred to in Article 67 clause 1 have been completed with a positive result, the state security service shall issue an industrial security certificate attesting that the business, scientific organisation or research-and-development organisation is capable of protecting classified information against any unauthorised disclosure.

Article 70.

Giving deliberately false information or withholding true information from the industrial security questionnaire, likewise defaulting on the obligation arising under Article 68 clause 3, shall constitute a basis for the industrial security certificate to be refused or revoked.

Article 71.

1. The refusal to issue an industrial security certificate shall not require any substantiation.
2. Unless important interests of the state should be thus put at risk, a representative of the business, scientific organisation or research-and-development organisation referred to in Article 65 clause 1 may familiarise himself or herself with the information collected in the course of the vetting proceedings, in particular with the data on the basis of which the refusal was made. The state security services shall advise the authorised entities of the said right.

Article 72.

The industrial security certificate and the refusal to issue an industrial security certificate shall at all times include:

- 1) an identification of the state security service which issued or refused to issue the industrial security certificate;
- 2) the place and date of issue;
- 3) the name and seat of the entity referred to in Article 65 clause 1;
- 4) the legal justification;
- 5) a statement that the industrial security certificate has been issued or refused; (and)

6) the name, seal and legible signature of the authorised civilian or military member of the state security service staff.

Article 73.

The Council of Ministers shall prescribe by Ordinance the specimens of:

- 1) the industrial security questionnaire;
- 2) the industrial security certificate; (and)
- 3) the refusal to issue an industrial security certificate.

Article 74.

The information collected in the course of the vetting proceedings referred to in Article 67 clause 1 shall be subject to protection, shall not be used for purposes other than that defined in this Act and releasing the same to other persons shall be forbidden.

2. The information referred to in clause 1 shall be made available exclusively at the request of the court or public prosecutor for purposes of a criminal prosecution, or to the President of the Republic of Poland or the Chairman of the Council of Ministers (when an important interest of the Republic of Poland so warrants).

3. Article 12 clause 1 of the Office for State Security Act shall apply to the information collected in the course of the proceedings referred to in Article 67 clause 1.

Article 75.

When classified information is generated in connection with the performance of the contract, regardless of the subject matter of the contract, the person referred to in Article 66 shall decide on according that information an appropriate security classification.

Article 76.

The provisions of this Chapter shall apply equally to those who take part in carrying out the contract, whatever their legal relationship with the business, scientific organisation or research-and-development organisation charged with performing the contract.

CHAPTER 12 MODIFICATIONS TO PROVISIONS IN EFFECT

Article 77.

In the 6 April 1990 Office for State Security Act (...)*, in Article 12 clause 1, the words , conducting the vetting proceedings pursuant to the classified information protection provisions are added after the word "criminal".

Article 78.

In the 28 September 1991 Treasury Revenue Inspection Act (...)*, in Article 34a clause 1 item 6, the period is replaced by a coma and the following item 7 is added:

7) the state security services and their military and civilian personnel duly authorised in writing, to the extent necessary to conduct the vetting proceedings pursuant to the classified information protection provisions.

Article 79.

In the 10 August 1994 Mental Health Protection Act (...)*, in Article 50 clause 2 item 3, the period is replaced with a coma and the following item 4 is added:

4) the state security services and their military and civilian personnel duly authorised in writing, to the extent necessary to conduct the vetting proceedings pursuant to the classified information protection provisions.

Article 80.

In the 14 December 1995 Office of the Minister of Defence Act (...)*, in Article 2, the following item 6a is inserted after item 6:

6a) general co-ordination of the activities concerned with the protection of classified information in the national defence department (of government),

Article 81.

In the 8 August 1996 Act on Work Organisation and Work Procedures of the Council of Ministers and on Ministers' Terms of Reference (...)*, in Article 39 clause 3 item 2j), the period is replaced with a coma and the following item 2k) is added:

k) protecting classified information.

Article 82.

In the 22 August 1997 Personal and Property Protection Act (...)* the following Article 35a is inserted after Article 35:

Article 35a. The security employee to be charged, pursuant to the 22 January 1999 Classified Information Protection Act (...)*, with the duties of a security officer or a member of the security service staff shall additionally meet the requirements set out therein.

Article 83.

In the 29 August 1997 Tax Law Act (...)*, in Article 297 paragraph 1, the period after sub-paragraph 6 is replaced with a coma and the following sub-paragraph 7 is added:

7) the state security services and their military and civilian personnel duly authorised in writing, to the extent necessary to conduct the vetting proceedings pursuant to the classified information protection provisions.

Article 84.

In the 29 August 1997 Banking Law Act (...)*, in Article 105 clause 1 item 2j) the period is replaced with a coma and the following item 2k) is added:

k) the state security services and their military and civilian personnel duly authorised in writing, to the extent necessary to conduct the vetting proceedings pursuant to the classified information protection provisions.

CHAPTER 13 INTERIM AND FINAL PROVISIONS

Article 85.

1. The head of the organisations shall appoint the security officers and organise the security services in the entities reporting to them within 3 months from the effective date of this Act and adjust the business premises to the requirements of this Act within 6 months from the effective date of this Act.

2. The security officers shall conduct a review of positions and prepare lists of the positions which involve access to classified information and of the persons allowed access to classified information.

Article 86.

1. Those documents generated between May 10, 1990 and the effective date of this Act which contain information being a state secret or public service secret and which have the "secret-special status", "secret" and "confidential" security classification accorded pursuant to the provisions in effect before this Act coming into force shall become, within the meaning of this Act, respectively, "top secret", "secret" and "confidential" documents.

2. The persons referred to in Article 21 clause 1 or their legal successors in respect to such documents containing state secret or public service secret information as were generated before May 10, 1990 shall, within 36 months from the effective date of this Act, review the said documents with the aim of adjusting their security classification to those appropriate under this Act. Pending (the review and adjustment), the said documents shall be understood to have such a security classification as is appropriate

under clause 1 unless separate provisions otherwise stipulate. Article 25 clause 5 shall apply, respectively.

3. After 36 months from the effective date of this Act those documents referred to in clause 2 which have not been reviewed shall become public(except for the documents meeting the specifications set out in Article 25 clause 2 item 1 and item 2. The latter shall henceforth become documents classified "top secret" and they shall be subject to protection pursuant to the above-quoted provision.

4. Clause 2 and clause 3 shall be without prejudice to the provisions of other Acts.

Article 87.

1. Subject to clause 2, those authorisations of access to state secret or public service secret information which have been issued pursuant to the provisions hitherto in effect:

1) to persons in positions subject to the special vetting proceeding requirement(shall become null and void after 12 months from the effective date of this Act;

2) to persons in positions subject to the extended vetting proceeding requirement(shall become null and void after 18 months from the effective date of this Act; (and)

3) to persons in positions subject to the standard vetting proceeding requirement(shall become null and void after 24 months from the effective date of this Act;

2. Article 44 clause 2 shall apply, respectively, to the persons referred to in clause 1.

3. Those decisions issued pursuant to the 14 December 1982 State and Public Service Secret Protection Act (...)* whereby the disclosure of information classified as a state secret or public service secret shall remain valid no later than December 31, 1999.

4. The authorisations issued pursuant to Article 16 of the Act referred to in clause 3 shall remain valid no later than December 31, 1999.

Article 88.

The heads of organisations may charge the in-house security services operating under separate provisions with duties and vest in them the powers of the security service according to the provisions of this Act.

Article 89.

1. The state secret or public service secret provisions issued pursuant to the Act referred to in Article 90 shall remain in force and effect for 12 months from the effective date of this Act unless they be contrary to this Act.

2. The state secret or public service secret provisions issued pursuant to other Acts shall be adjusted to the requirements of this Act within 12 months from the effective date of this Act.

Article 90.

The 14 December 1982 State and Public Service Secret Protection Act (...) * is hereby rendered null and void.

Article 91.

This Act shall come into force after 30 days from its promulgation.

President of the Republic of Poland: A. Kwaśniewski

* * *

(to be continued in the next issue)

(...)* The particulars of Dziennik Ustaw issues in which the cited law and subsequent amendments thereto were published are not quoted in this text.

Copyright 1-99 Polish News Bulletin
Polish News Bulletin
26 May 1999 21-99

SECTION: Law Supplement
LENGTH: 6907 words

HEADLINE: THE CLASSIFIED INFORMATION PROTECTION ACT of 22 January 1999 (Part IV)

BODY: ANNEX NO 1: STATE SECRET CLASSIFIED INFORMATION

I. Information classified "top secret"

1. Information concerning external military threats to the security of the state; defence plans and forecasts and the decisions and tasks resulting therefrom.
2. The structure, organisation and functioning of the system for governing the state and commanding the Armed Forces in times of threat to the state and in wartime.
3. The location, equipment, protective potential and organisation of the system for defending the command centres from which the state is to be governed and the Armed Forces commanded in times of threat to the state and in wartime.

4. The organisation and functioning of the communications systems for governing the state and commanding the Armed Forces during times of increased defence readiness and in wartime.
5. The central mobilisation programme for the national economy.
6. Information concerning the planning, organisation and functioning of the Armed Forces' mobilisation deployment plan.
7. The detailed structure of the Armed Forces, likewise of wartime military districts and types of force.
8. Information concerning: the Armed Forces' combat effectiveness; the various military districts and types of force; and the potential enemy in the forecast areas and directions of warfare.
9. The combat tasks of the Armed Forces and operational groupings.
10. The organisation and functioning of the national air and anti-aircraft defence system.
11. The organisation, deployment, tasks and operational capacity of the radio-electronic reconnaissance and combat system.
12. The planning and execution of projects concerned with operational camouflaging of forces.
13. The planning, execution and findings of scientific research and research-and-development projects of special importance to national defence and security.
14. Passwords and codes giving access to facilities in which or with the aid of which information classified "top secret" is stored, processed and transmitted.
15. The communications systems planned, organised and maintained by the communications service reporting to the ministers responsible for internal affairs and public administration, to the Minister of Defence and to the Chief of the Office for State Security.
16. The organisation, functioning, security arrangements and facilities for cryptographic protection of the transmission of information classified "top secret", likewise coded messages secured by code algorithms for protecting information accorded that secrecy classification.
17. The organisation, forms and operational work methods of the state bodies, services and institutions authorised to engage in operational-reconnaissance activities.
18. The detailed directions of operational work and interests of the state security services.

19. The detailed organisational and manpower structure of those entities and structures within the state bodies, services and institutions referred to in item 17 which engage in operational-reconnaissance activities, likewise systems for registering information relating to the civilian and military personnel of the said entities and structures.
20. The particulars which reveal or are capable of revealing the identity of members of the civilian and military personnel authorised to engage in operational-reconnaissance activities and employed in the state bodies, services and organisations referred to in item 17.
21. The particulars which reveal or are capable of revealing the identity of those persons who, while not members of the civilian and military personnel of the state bodies, services and organisations referred to in item 17, have assisted the said structures in their operational-reconnaissance activities.
22. Information relating to those documents which prevent the disclosure of particulars by which the identity of members of the civilian or military personnel of the state bodies, services or institutions referred to in item 17 might be established or means employed by them in their operational-reconnaissance work identified.
23. Information relating to the following investigative techniques the use of which is permitted by statutes: technical means of covert intelligence gathering and evidence recording; surveillance of correspondence; controlled purchase; and covertly monitored dispatch.
24. Plans concerning the procurement of special investigative-technique equipment and stocks of the same at the state bodies, services and institutions referred to in item 17.
25. Intelligence and things secured by applying technical means of covert intelligence gathering and evidence recording and through surveillance of correspondence.
26. Information relating to operational-reconnaissance activities--whether planned, in progress or executed--of the state bodies, services and institutions referred to in item 17, likewise such intelligence and objects secured through those activities by which the persons who have assisted the said bodies, services and institutions in their operational-reconnaissance activities might be identified.
27. Reports, bulletins, information and statistical data relating to operational activities of the state bodies, services and institutions referred to in item 17.
28. The management of budgetary funds and state property assigned to special purposes.
29. The organisation, functioning and technical means of radio-counterintelligence protection of state security.

30. The classified information accorded the "TOP SECRET" or an equivalent secrecy classification which is exchanged between the Republic of Poland and the North Atlantic Treaty Organisation, European Union, Western European Union and other international organisations and states.

II. Information classified "secret" for reasons of national defence and security of the state and for reasons of public order:

1. The planning, deployment and condition of state reserves.
2. Departmental- and voivodship-level mobilisation programmes for the national economy.
3. National and voivodship-level civil defence plans.
4. Guidelines on the financial system of the state in times of increased defence readiness and in wartime.
4. The deployment, manpower and equipment of military units--to the extent not covered by the Treaty on Conventional Forces in Europe (CFE).
6. The detailed structure of the Armed Forces, likewise of military districts and kinds of force.
7. Plans and forecasts for organisational and technical development of the Armed Forces and individual services thereof.
8. The location, kind and designated purpose, likewise technical-protective qualities of special civil engineering structures.
9. The organisation of comprehensive arrangements for a uniform state telecommunications network to serve defence purposes.
10. Information concerned with the designing, laying down, management and running of telecommunications, electronic and postal systems and networks for the transmission of state secret classified information by the Armed Forces, state security services and public administration--to the extent necessary to render those systems and network secure.
11. Summary intelligence on the defence industry's special output, likewise development forecasts, plans and production and service potentials of businesses, scientific organisations and research organisations--to the extent that such information concerns the fulfilment of orders for weaponry and military equipment.
12. Military special maps and photographic documents representing engineering land development sites and projects in the forecast areas and directions of warfare.

13. Collections of geodesic coordinates or rectangular landmarks in areas of substantial importance to the defence potential and security of the state.
14. Photogrammetric and tele-detection materials obtained by aerial and land mapping of sites and areas of material importance to the defence potential and security of the state.
15. Geodesic and cartographic materials containing information on the location, kind, nature or purpose of facilities of material importance to the defence potential and security of the state.
16. Information relating to the conversion of the national economy to defence purposes in times of increased defence readiness or in wartime.
17. Information concerning the preparation, organisation and use of rail, road and water transport and the protection of transport facilities in times of increased defence readiness or in wartime.
18. The organisation and functioning of military alert systems and the tasks of military units and garrisons in the process of achieving higher stages of combat readiness.
19. Tasks of the central constitutional bodies of the state, ministers, central administrative agencies and voivods in the process of the putting the state on higher stages of defence readiness.
20. The organisation and functioning of the system for supplying the Armed Forces with weaponry, military equipment and ammunition in the process of achieving higher stages of combat readiness.
21. The system for registering information about those in positions relating to the defence potential of the state.
22. Information concerning the Penitentiary Service units' security and defence system in times of increased national defence readiness or in wartime.
23. Arrangements for protecting, in the event of war, cultural assets of special importance to the national cultural heritage.
24. Data on the Ministry of Internal Affairs' physical war reserves.
25. Detailed data on those organisational arrangements, methods and means of protecting the state secrets which, if disclosed, might become ineffectual.
26. Information on the planning, deployment, purpose and equipment of special facilities and sites and plans for the defence and protection thereof.

27. Detailed data on the persons suspected of engaging in activities prejudicial to the security, defence potential, independence, wholeness or international position of the state, or of terrorist activities, obtained and processed by the state security services.

28. The detailed organisational and manpower structure of the various services of the Office for State Security, Military Information Services, Police, Frontier Guard Service and of the military units reporting to the minister responsible for internal affairs, unless such materials contain information with a higher secrecy classification.

29. The system for registering data concerning civilian and military personnel of the Office for State Security, Military Information Services, Police, Frontier Guard Service and of the military units reporting to the minister responsible for internal affairs, likewise the data so registered, unless such materials contain information with a higher secrecy classification.

30. Statistical data concerning personnel matters of the state security services, except for the data stated in the Budget Act.

31. Information derived from archival materials on operational activities, including index files and briefs prepared on the basis of operational archival materials, unless such materials contain information with a higher secrecy classification.

32. The system and manner of protecting the state borders, of monitoring cross-border traffic, anti-terrorist and anti-sabotage measures, likewise information on the operational potential for protecting the state borders.

33. The detailed forms and methods of operation by the Office for State Security, Military Information Services, Police, Frontier Guard Service and of the military units reporting to the minister responsible for internal affairs, unless such materials contain information with a higher secrecy classification.

34. Information on operational-reconnaissance activities-- whether planned, in progress or completed--of the state bodies, services or institutions authorised to engage in the same and the intelligence and things secured as a result of those activities, unless such materials contain information with a higher secrecy classification.

35. Detailed information on the functioning of the system for protecting classified information which has the status of a state secret.

36. Logs in which incoming and outgoing documents are registered and registers of other materials containing classified information with the status of a state secret.

37. Detailed information concerning the protection and security of facilities and sites of importance to the national economy or to the defence potential or security of the state.

38. Those detailed data on investigative-surveillance operations--whether planned, in progress or completed--the disclosure of which might obstruct the legitimate progress of criminal proceedings.

39. The inventions which are classified as secret pursuant to the inventions provisions.

40. The information with the "SECRET" or an equivalent secrecy classification which is exchanged between the Republic of Poland and the North Atlantic Treaty Organisation, European Union, Western European Union and other international organisations and states.

III. Information classified "secret" for reasons of important national interests:

1. Materials prepared for the Council of Ministers concerning the strategic potential of the state and strategic government orders and the execution thereof.

2. Those instructions concerning negotiations on the conclusion of financial agreements of national importance the disclosure of which might affect the further course of the negotiations.

3. Those motions for the granting of surety and those surety contracts and contracts for the granting of surety with concern producers of defence equipment.

4. The system for ensuring the security of money in the state banks and in money-printing and coin-minting institutions.

5. The National Bank of Poland's special domestic money reserve limit.

6. Information relating to the organisation and security arrangements for transporting sums of money in excess of 500 thousand EURO, as maintained by the state banks and money-printing and coin-minting institutions.

7. The system for ensuring the security of excise tax stamps in the institutions printing those stamps and in the state banks and Treasury Revenue Inspection offices.

8. Information relating to the designing of money and preparing the production thereof, except for the collector-item coins, Treasury and National Bank of Poland securities and excise tax stamps--to the extent necessary to prevent counterfeiting or alteration of money prior to its being put into circulation.

9. Information relating to the technology of manufacturing notes and coin, revenue stamps, excise stamps, securities and credit cards issued by the Treasury or the National Bank of Poland or other state banks.

10. Information relating to the manufacturing technology and detailed methods of securing (against forgery) identity cards and other secured documents issued by public authorities.
11. The National Bank of Poland's decisions on one-off revision of the exchange rate of the zloty relative to foreign currencies (devaluation, appreciation)--pending public announcement thereof.
12. The state banks' protection and security plans, directives and arrangements.
13. The National Bank of Poland's interest rates, pending public announcement thereof.
14. The zloty's divergence band from the central exchange rate, pending public announcement thereof.
15. The research-and-development projects of particular importance to economic interests of the state which have been commissioned by ministries and central agencies of the government.
16. Information concerning technical, technological or organisational arrangements and methods--insofar as the disclosure thereof would be injurious to important interests of the state.
17. Information on the manner of operation of the monitoring-alert devices and alarm systems which secure access to the sites and facilities where Grade I and II nuclear materials are stored and used.
18. Information relating to those foreign policy plans and tasks the disclosure of which would be injurious to important interests of the state or of another party to international relations, pending official announcement thereof.
19. Materials, documents and reports on international negotiations and consultations, likewise international agreements or sections thereof, if accorded the classified information status at the request of one of the parties.
20. Political, economic or military information concerning other states, if obtained on the condition that its secrecy will be ensured.
21. The organisation and functioning of the diplomatic mail system.
22. The system for protecting Polish diplomatic and consular missions.
23. The wartime tasks of Polish diplomatic and consular missions.
24. The tasks concerned with protecting foreign diplomatic and consular missions in the Republic of Poland in wartime.

25. Plans, forecasts and information concerning the expansion of foreign trade in special equipment and arms and in special technology and services.

26. The classified information with the "SECRET" or an equivalent secrecy classification which is exchanged between the Republic of Poland and the North Atlantic Treaty Organisation, European Union, Western European Union and other international organisations and states.

ANNEX NO 2. PERSONAL SECURITY QUESTIONNAIRE

Madam/Sir,

The Government of the Republic of Poland, bearing in mind the interests of national security and committed to protecting the same, presents this questionnaire confident that you will fill it according to your best knowledge and will. Rest assured that your cooperation will be appreciated and that this questionnaire will serve no other purposes than that of protecting national security against threats from foreign special services, terrorist groups, or criminal groups. Please read the enclosed instructions carefully and, when in doubt, ask your organisation's security officer or the appropriate state security service for assistance.

Instructions:

1. Read the questionnaire carefully before filling.
2. Write in block letters or, if possible, typewrite.
3. Where not enough space is available, write on a separate A-4 sheet and enclose it to the questionnaire.
4. Write "Don't know" whenever you cannot supply the required data due to the lack of knowledge.
5. Write "Not applicable" whenever an item or sub-item of the questionnaire does not concern you.
6. Write "See item/sub-item" whenever particulars requested under consecutive items are identical with those stated previously.
7. If any of your family members referred to in items 2-9 of the questionnaire is dead, please fill only his/her given name and surname, date of birth and the word "deceased" in the respective section.
8. You are requested to answer this questionnaire to the extent stated below in connection with (proceedings on) authorising your access to classified information:

9. The persons subject to vetting proceedings in connection with access to information classified "restricted" are requested to answer the following items: 1, 2a-c, 3a-c, 12, 13, 22, 28a.
10. The persons subject to vetting proceedings in connection with access to information classified "confidential" are requested to answer only the following items: 1-7, 9, 12, 13, 15-19, 22-28, 30, 32 and 33.
11. The persons subject to vetting proceedings in connection with access to information classified "secret" do not answer item 31.
12. The persons subject to vetting proceedings in connection with access to information classified "top secret" are requested to answer all the items.
13. Where the questionnaire is filled for purposes of a repeated vetting proceeding conducted after 10 years, the person who received a security clearance authorising his/her access to information classified "confidential" is requested to answer items 10, 17, 22-25, 28 and 29, solely in respect to the period from the date of filling the previous questionnaire to the date of filling the next one. Write "no change" whenever the particulars covered in the above mentioned items have not changed.
14. Whenever the questionnaire is filled for purposes of repeated vetting proceedings conducted after 3 years in respect to a person who received a security clearance for access to information classified "top secret" and after 5 years in respect to a person who received a security clearance for access to information classified "secret", the respondent shall not answer items 1j and 1k
15. Whenever the questionnaire is filled for purposes of consecutive vetting proceedings conducted after the above mentioned periods of time, the respondent is requested to answer items 10, 17, 22-25, 28 and 29 solely in respect to the period from the date of filling the previous questionnaire to the date of filling the next one. Write "no change" whenever the particulars covered in the above mentioned items have not changed.

THE PERSONAL SECURITY QUESTIONNAIRE (the written text only)

This personal security questionnaire is to be used in any manner permitted by law for purposes of vetting proceedings conducted in connection with your permit to have access to information with the secrecy classification (mark the appropriate block):

"Restricted"

"Confidential"

"Secret"

"Top secret"

1. The investigated person:

a. Surname

b. Previous surnames (including the family name)

c. Given names

d. Previous given names (if changed)

e. Date of birth, place of birth

f. Present citizenship(s)

g. Former citizenships

h. If you changed your citizenship, please state:

- the given names and surname stated in the deed of change or forfeiture of your foreign citizenship or in the deed of granting your present citizenship

- the date of issue

- the number and name of the (deed) document

- the issuing authority

i. Identity card:

series and number

the issuing authority

issued on

j. PESEL number

k. Taxpayer Identification Number (NIP)

l. Military rank

l/.Military service document:

series and number

the issuing authority

issued on

m. Present permanent registered address

(country, town, street, house number, apartment number)

n. Present temporary registered address (if different from that given in item 1m)

o. Passport:

series and number

the issuing authority

issued on

valid to

p. Present employment/service

1. The employer's name and REGON number, address(country, town, street, house number, postal code, phone and fax number); position held or nature of work performed; monthly wages/income after ta

X2. (ditto)

r. Additional sources of livelihood/earnings

(including incomes other than earned, such as pensions received from abroad, dividend on securities owned, interest on bank deposits, capital gains on stock exchange transactions, trust fund units, property lease incomes, game of chance winnings in excess of an equivalent of three average (monthly) wages in Poland, author's fees, teaching fees, incomes from agency contracts, and the like).

1. The employer's name and REGON number, address (country, town, street, house number, postal code, phone and fax number); position held or nature of work performed, monthly wages/incomes after ta

X2. (ditto)

3. Other incomes (source, amount)

2. Father of the investigated person:

a) Given name and surname

b) Place of birth, date of birth

c) Citizenship(s)

d) Present employment

1. The employer's name and REGON number, address (country, town, street, house number, postal code, phone and fax number); position held

e) Present registered address (for permanent and temporary residence)

(country, town, street, house number, apartment number, postal code, home phone number)

f) Present place of abode (if different from that given above)

(country, town, street, house number, apartment number, postal code, home phone number)

3. Mother of the investigated person

a) Given name and surname, family name

b) Place of birth, date of birth

c) Citizenship(s)

d) Present employment

1. The employer's name and REGON number, address (country, town, street, house number, postal code, office phone and fax number); position held

e) Present registered address (for permanent and temporary residence)

(country, town, street, house number, apartment number, postal code, home phone number)

f) Present place of abode (if different from that given above)

(country, town, street, house number, apartment number, postal code, home phone number)

4. Siblings of the investigated person

1)

a) Given name and surname, family name

b) Place of birth, date of birth

c) Citizenship(s)

d) Present employment

The employer's name and REGON number, address (country, town, street, house number, postal code, office phone and fax number); position held

e) Present registered address (for permanent and temporary residence)

(country, town, street, house number, apartment number, postal code, home phone number)

f) Present place of abode (if different from that given above)

(country, town, street, house number, apartment number, postal code, home phone number)

2)(ditto)

3)(ditto)

5. Spouse of the investigated person

including the person with whom the person referred to in item 1 cohabitates and maintains household)

Given name and surname (also family name)

Place of birth, date of birth

Citizenship(s) Present employment

a) The employer's name and REGON number; address (country, town, street, house number, postal code, office phone and fax number); position held

b) (ditto)

Present registered address (for permanent and temporary residence, if different than that given in item 1m or 1n) (country, town, street, house number, apartment number, postal code, home phone number)

Present place of abode (if different from that given above) (country, town, street, house number, apartment number, postal code, home phone number)

Date and place of contracting marriage

Identity card:

series and number

the issuing authority

issued on

6. Father of the person referred to in item 5:

Given name and surname

Place of birth, date of birth

Citizenship(s)

Present employer(s)

The employer's name and REGON number, address (country, town, street, house number, postal code, office phone and fax number); position held

Present registered address (for permanent and temporary residence) (country, town, street, house number, apartment number, postal code, home phone number)

Present place of abode (if different from that given above) (country, town, street, house number, apartment number, postal code, home phone number)

7. Mother of the person referred to in item 5:

Given name and family name

Place of birth, date of birth

Citizenship(s)

Present employer(s)

The employer's name and REGON number; address (country, town, street, house number, postal code, office phone and fax number); position held

Present registered address (for permanent and temporary residence) (country, town, street, house number, apartment number, postal code, home phone number)

Present place of abode (if different from that given above) (country, town, street, house number, apartment number, postal code, home phone number)

8. Siblings of the person referred to in item 5:

(a) Given name and family name

Place of birth, date of birth

Citizenship(s)

Present employer(s)

The employer's name and REGON number; address (country, town, street, house number, postal code, office phone and fax number); position held

Present registered address (for permanent and temporary residence)

(country, town, street, house number, apartment number, postal code, home phone number)

Present place of abode (if different from that given above)

(country, town, street, house number, apartment number, postal code, home phone number)

(b) (ditto)

9. Children of the persons referred to in item 1 and item 5

(a) Place of birth, date of birth

Surname

Given name (names)

Present registered address (for permanent and temporary residence), if other than given in item 1m or 1n or item 5

(country, town, street, house number, apartment number, postal code, home phone number)

Present place of abode (if different from that given above)

(country, town, street, house number, apartment number, postal code, home phone number)

Present employment

The employer's name and REGON number; address (country, town, street, house number, postal code, office phone and fax number); position held

(b)(ditto)

(c)(ditto)

10. If any of the family members referred to in items 2-9 reside permanently abroad or (at any time) stayed abroad for more than 3 months, please enter the following particulars:

Period of residence or stay:

Surname and given name

Country and full address

Reasons for staying abroad

from-to

11. Were you (at any time) between 1944-1990 an employee, servant or covert collaborator of state security services within the meaning of the 11 April 1997 Act on Disclosure of 1944-1990 Employment, Service or Collaboration with State Security Services by Persons in Public Office (...)*?:

Yes

No

Not applicable

12. Have you been punished by law in the recent 10 years and by what authority (if affirmative, please state by which authority and for what offence or misdemeanour)?

13. Are you aware of penal proceedings being in progress against you for an offence or misdemeanour?

(If affirmative, please state the body in charge of the case and, where possible, the registration number of the case)

14. Have you ever suffered from mental diseases or other mental capacity-disturbing ailments? If affirmative, please state the disease, periods of illness and the health service facility or doctor who attended or is attending you in connection with the above mentioned ailments or disease.

(a)

(b) 15. Have you ever taken narcotics or other mind-affecting drugs? If affirmative, please state what drugs, when, and whether you still engage in such practices. Do not include the occasions when narcotics or mind-affecting drugs were administered to you by duly authorised physicians unless such treatment resulted in your continued dependence on the like substances.

16. (a) Have you, in the recent 10 years, indulged in consuming alcohol in quantities resulting in a disturbance or loss of mental faculties? If affirmative, please state how often, in what circumstances, and whether you have been treated in that connection at a specialist counselling or health care facility (state the full name and address of the facility)

(b) Has the drinking of alcohol ever caused problems in your career or personal life?

17. Please state your career (service) record in the recent 10 years:

Period (from-to)

Employers' full name and address

Position last held

18. Are you, your spouse, or other members of your household in debt to individuals or corporations (loans, credits and the like) in excess, cumulatively, of six times your (monthly) remuneration? If affirmative, please state the debtor, debt amount, creditor, title and planned repayment date:

(a)

Surname and given name

Type of liability

Amount of liability

Creditor

Title

Repayment date

(b) (ditto)

(c) (ditto)

19. Do you, your spouse, or other members of your household have other outstanding financial commitments (e.g. tax arrears, alimony or child support payments, repayment of a hypothec-secured loan, lien, liabilities arising from court verdicts)? If affirmative, please state the debtor, debt amount, creditor, title and planned repayment date.

(a)

Surname and given name

Type of liability

Amount of liability

Creditor Title

Repayment date

(b)(ditto)

(c)(ditto)

20. Please state the incomes you, your spouse and other members of your household had in the year preceding the filling of this personal security questionnaire. (a)

Surname and given name Net income

(b)(ditto) (c) (ditto)

21. Do you, your spouse or other members of your household own real property, a business, or shares in another's business. If affirmative, please name the person and state the kind and location of the property or business:

(a)

Surname and given name

Property, business, or shares

Location

(b) (ditto)

(c) (ditto)

22. Have you even been permitted to have access to classified information with the status of a state secret, whether in Poland or another country? If affirmative, please give the following particulars:

Full name and address of the institution in which your access to that information was authorised

Country

Scope and secrecy classification of the information to which you had access

Period (from-to)

23. Have you ever resided abroad for more than 10 days, including on business, after your 18th birthday? If affirmative, please give the following particulars:

Period of residence

Country, town, house and apartment number, postal code

Reasons for staying abroad

24. Have you ever entered into a gainful occupation while abroad? If affirmative, please fill in the following particulars:

Period

(from-to)

Country, employer's full address

Position held

Kind of work performed and income earned

25. Please give your residence record in the recent 10 years (in Poland and other countries)

Period of habitancy or registered residence

(from-to)

Country, location (voivodship, powiat, gmina) postal code

Address: street, house number, apartment number

26. Please state the particulars of the persons currently sharing your premises (e.g. members of family, sub-tenants, the owner of the premises)

Surname and given name

Place and date of birth

27. Who owns the premises you currently reside in (institution/firm or individual--the full address and phone number)

28. (a) Your education (higher, secondary, primary) and professional credentials or academic degrees held;

(b) The higher educational establishments, schools and vocational courses you attended and finished in past:

Attendance period

Names and addresses of higher educational establishments, schools and vocational courses

Diplomas, graduation certificates

29. Have you or any of the members of your family referred to in items 2-9 maintained, in the recent 20 years, business or personal contacts with citizens of other states? If affirmative, please fill in the following particulars:

Period (from-to)

Person-contact

Country, full address

Reasons for/nature of contacts

30. Have you ever been a member of Polish or foreign organisations, political parties, or associations, registered or otherwise?

Organisation: name and full address

Function performed

Membership period

31. Please give as your reference 3 persons who have known you for 2 years or longer (other than the family members referred to in items 2-9, those attending to your business matters, or those who have a confidential relation with you for reasons of professional practice).

Given name and surname

Employment

Full home address and phone number

32. Have you ever, while abroad, been questioned or otherwise encouraged by foreign authorities (immigration, inland revenue or others) to speak on subjects relating to national security and defence? To your knowledge, has your spouse, a member of your household or of your family been approached in a similar way? If affirmative, mark the appropriate block. Do not fill in any details; these shall be discussed with you by the representative of the state security services in charge of the vetting proceeding.

Yes

No 33. Have you ever found yourself a target of foreign special services' or other foreign prosecuting institutions' (Police, Border Guard Force), or organised crime groups' (whether Polish or foreign) interest? To your knowledge, has your spouse, a member of your household or of your family been approached in a similar way? If affirmative, mark the appropriate block. Do not fill in any details; these shall be discussed with you by the representative of the state security services in charge of the vetting proceeding.

Yes

No

- - - I hereby declare that I have filled this questionnaire to the best of my knowledge, aware that any false statement or any omission of a pertinent fact will constitute a sufficient reason for discontinuing the vetting proceedings and that my security clearance may be refused on these grounds.

I hereby declare that I agree to submit to the vetting proceedings conducted pursuant to the 22 January 1999 Classified Information Protection Act (...)* and Article 7 item 5 of the 29 August 1997 Personal Information Protection Act (...)*; I agree to having my personal data stated in this questionnaire processed within the meaning of Article 7 item 2 of the above mentioned Act, subject to the respective limitations arising under the cited Classified Information Protection Act.

Number of sheets appended to this questionnaire:

Signature of the respondent answering the questionnaire for purposes of a vetting proceeding

Place

Date

- - -

Legible signature and seal of the organisation head and security officer

Place

Date

* * *

(...)* The particulars of Dziennik Ustaw issues in which the cited law and subsequent amendments thereto were published are not quoted in this text.

Source: Dziennik Ustaw No 11, 8 February 1999

The PNB is a non-profit organization publishing a daily digest of the Polish press. No legal responsibility is accepted for any errors or omissions or misleading statements, however caused, in either source or final texts. Copyright: PNB 1999 LANGUAGE: ENGLISH LOAD-DATE: May 26, 1999