THE STATE REGISTRY OF LEGAL ACTS OF THE REPUBLIC OF AZERBAIJAN

Type of act	*Resolution of the Central Bank of the Republic of Azerbaijan*
Date of adoption	*28.10.2014*
Registration #	*24/2*
Title	*on approval of the Regulations on Issuance of Permits for and Oversight of the Processing Activity*
Source of official publication	
Effective date	*12.11.2014*
Index code on Unified Legal Classification of the Republic of Azerbaijan	*090.060.010*
Registration # of the State Registry of Legal Acts	*23201410280242*
Date the legal act was included to the State Registry of Legal Acts	*11.11.2014*

In order to align the normative act of the Central Bank of the Republic of Azerbaijan of legal nature to the Law of the Republic of Azerbaijan on Regulation of Entrepreneurial Reviews and Protection of Interests of Entrepreneurs, as well as strengthen requirements on reliability and security of the processing activity, based upon Articles 22.0.17 and 44 of the Law of the Republic of Azerbaijan on the Central Bank, the Management Board of the Republic of Azerbaijan

DECIDES to:

1. approve the Regulations on issuance of permit for and oversight of the processing activity (annexed).
2. annul the Regulations on Issuance of Permits for Processing Entities and Oversight of Processing Activity approved at resolution of the Management Board of the Republic of Azerbaijan dated 09.09.2009 (Minutes # 26) (certification 3469 dated 23.09.2009).
3. assign the Legal department (R.Malikova) to ensure submission of this Resolution to the Ministry of Justice of the Republic of Azerbaijan to be entered to the State Registry of Legal Acts of the Republic of Azerbaijan within 3 days.

Chairman **Elman Rustamov**

'Approved'

The Central Bank

of the Republic of Azerbaijan

Protocol # 26

Resolution # 24/2

28 October 2014

REGULATIONS ON ISSUANCE OF PERMITS FOR AND OVERSIGHT OF THE PROCESSING ACTIVITY

1. General Provisions

These Regulations have been developed according to Article 44 of the Law of the Republic of Azerbaijan on the Central Bank and Article 32 of the Law of the Republic of Azerbaijan on Banks and establish rules on issuance of permits for service centers to provide a processing activity and oversight over the activity therein, and minimum requirements on the reliability and security of the processing activity.

2. Definitions

2.1. The definitions used in these Regulations shall bear the following meanings:

2.1.1. **processing activity** – collection, processing and transfer of data on payment card operations, as well as maintenance of card issue and acquiring;

2.1.2. **service center** – legal entity, entitled to provide a processing activity under these Regulations;

2.1.3. **transaction** – full or partial payment for goods, work and services, inter-account transfers, exchange of currency and cash disbursement via payment cards;

2.1.4. **high security zone** – the area, where workstations (rooms) for server equipment dedicated for the processing activity, production, storage and handover of payment cards, printing of PIN-envelopes, embedding chip on a card, personalization of the payment card or development of necessary data to that end are located;

2.1.5. **specific waste** – damaged and unfit cards, materials used in card production and/or during personalization;

2.1.6. **personalization** –uploading cardholder data to an electronic carrier (chip) and/or magnet tape when developing payment cards and printing of identification data via embossing or engraving.

3. Permit issuance

3.1. The legal entity shall submit the following documents and data signed by the head of the executive body to the Central Bank in order to obtain a permit for a processing activity:

3.1.1. application to obtain a permit, compiled under the requirements of Article 30 of the Law of the Republic of Azerbaijan on Administrative Execution;

3.1.2. notarized copies of the state registration document and the Charter;

3.1.3. form, filled in by the manager of the service center's executive body (Annex 1) and

notarized copy (copies) of his/her educational credential(s);

3.1.4. list of major equipment used for the processing activity (servers, other equipment required for production, and personalization of payment cards, and for the processing activity);

3.1.5. the list of major software to carry out a processing activity;

3.1.6. topological diagram on interrelation between software specified in Item 3.1.5 and equipment in use under Item 3.1.4 herein;

3.1.7. layout of the area (premises), where the processing activity will be carried out (to indicate location of rooms, surveillance cameras, on-door mounted card readers, seismic and motion detectors, fire protection, alarm systems);

3.1.8. business continuity plan of the processing activity in emergency situations (to indicate restoration of the processing activity in the premises, the service center is located in, organization of the efforts on transfer to the Back-up Center, and staged actions on restoration of the activity);

3.1.9. information on self-assessment (Annex 2);

3.2. The documents and data submitted to obtain a permit for a processing activity shall be reviewed under the Law of the Republic of Azerbaijan on Administrative Execution.

3.3. The permit shall be issued for an unlimited time.

3.4 The permit for a processing activity shall be issued under the following terms and conditions:

3.4.1. full submission of documents and data specified for obtaining a permit under these Regulations;

3.4.2. lack of inaccurate or distorted data in submitted documents;

3.4.3. the head of the executive body has a higher education;

3.4.4. self-assessment data (Annex 2) are approved to meet the requirements of Item 4 herein.

4. Minimum requirements on the processing activity

4.1. requirements on Information technologies (IT systems):

4.1.1. only related responsible persons should be authorized to develop personalization data and have access to the network designated for personalization and external interventions to the network should be prevented.

4.1.2. personalization files should be deleted from the memory of relevant devices immediately upon personalization of cards. The person responsible for information security should verify and document the deletion of these files no less than once a quarter.

4.1.3. all external hard disks (USB, diskettes, discs) deployed within the high security zone

should be marked, their utilization controlled and stored safely. Responsible persons should be designated on storage and use of the devices in question.

4.1.4. external hard disks with data may be taken out or brought into the high security zone and registered only by related responsible persons.

4.1.5. the service center should have a topological diagram of the network reflecting all system components. The network's system component should be adjusted to the existing situation.

4.1.6. the existing configuration of network equipment and all modifications should be documented.

4.1.7. all internal high security zone networks, global and local networks should be separated by network protectors. Parameters of network protectors and relevant network equipment may be modified by the designated responsible person.

4.1.8. all computers and servers should have licensed anti-virus programs installed. To protect systems and software from all possible and potential viruses the anti-virus software should be updated on an ongoing basis.

4.1.9. wireless network may not be used to transfer personalization data. To prevent data transfer the person responsible for information security should take actions to discover hidden wireless networks and prevent data transfer through them.

4.1.10. the service center should conduct penetration tests no less than once a year or immediately after modifications to network configuration. Test results should be documented and the head of the service center should keep elimination of revealed gaps under control.

4.1.11. the service center should have procedures in place addressing the order of generation, usage, updating, delivery and cancellation of user passwords.

4.1.12. in order to maintain a reliable and ongoing performance of IT systems in emergency situations the service center should create a Back-up Center to store back-up copies outside the center.

4.1.13. to verify maintenance of IT systems reliable and ongoing performance in emergency situations the service center should carry out a processing activity over the Back-up Center no less than once a year and inform the Central Bank within the timeframe specified in Item 5.4. herein.

4.2. Requirements on security of the area (building), the processing activity will be carried out:

4.2.1. the area (building) should be equipped with fire protection systems, including fire extinguishers in a good working condition.

4.2.2. surroundings, indoor perimeter, entrance and exits should be equipped with surveillance cameras capable to clearly capture images any time of a day. Recordings of surveillance

cameras should be kept by the security service for 6 (six) months.

4.2.3. all external walls, windows, doors and other entrances should be equipped with seismic, motion or connection detectors to prevent external intrusion.

4.2.4. All entries to and exits from the area (building) should meet the following requirements:

4.2.4.1. the security service should provide 24-hour control;

4.2.4.2. doors should be closed to prevent external intrusion;

4.2.4.3 entrance doors should be equipped with a card reader access system, that activates closing mechanisms;

4.2.4.4. access doors to the area (building) should be opened via a special algorithm (e.g. if one door is opened by an employee to enter the area, the other one should be opened by an employee of the security service.);

4.2.4.5. external emergency exits should be equipped with local alarm signals;

4.2.4.6. on-door mounted alarm signals should be checked by the security service once a month and documented;

4.2.4.7. Illuminated boards and emergency lighting installed in entrances should be checked by the security service once a month and results documented;

4.2.4.8. all entries and exits, the surrounding of the building (area) the service center is located in, in the vicinity of no less than 2 m should be clearly illuminated in the dark time of a day (from sunset to sunrise).

4.2.5. The room of the security service should meet the following requirements:

4.2.5.1. two telephone lines, motion detectors, a signaling system, surveillance cameras, hidden buttons for alarm, direct communication with police and fire fighting service should be supplied.

4.2.5.2. the door should be equipped with card readers with only access by security service employees.

4.2.5.3. it should be located outside the high security zone.

4.2.5.4. if not an integral part of the building (area), should be constructed of resilient materials (stone, brick, concrete).

4.2.5.5. the door should be permanently closed, if left open for over 30 sec, alarm should activate.

4.2.6. All rooms located in the high security zone should meet the following requirements:

4.2.6.1. access to the high security zone should be equipped with a door or device (lock chamber) opened via a dedicated algorithm (e.g. to enter the area if one door is open, the next door should not open and also two separate employees should not be able to enter simultaneously).

4.2.6.2. rooms should be supplied with fire-proof furniture.

4.2.6.3. should be constructed of resilient materials (stone, brick, concrete).

4.2.6.4. should be supplied with surveillance cameras capable to capture the entire area simultaneously. Recordings of surveillance cameras should be stored at least for 6 (six) months.

4.2.6.5. doors of rooms should be supplied with alarm signals.

4.2.6.6. if the doors of rooms are left open for over 30 sec, the alarm signal should activate.

4.2.6.7. entry to and exit from rooms should be managed by on-door card readers.

4.2.6.8. the entire area should be supplied with motion detectors.

4.2.6.9. the doors of the rooms should be always locked.

4.2.6.10. rooms should be supplied with workable fire protection systems, including fire extinguishers.

4.2.6.11. if any, all exterior windows should be iron barred or supplied with bullet-proof glass.

4.2.7. The warehouse should be strictly protected and meet the following requirements along with sub-item 4.2.6. herein:

4.2.7.1. it should be supplied with iron bars internally.

4.2.7.2. the floor, the ceiling and all walls should be supplied with seismic detectors to protect from external intrusion.

4.2.7.3. cards stored in the warehouse should be inventorized on a monthly basis and results documented.

4.2.7.4. 2 card readers need to be used simultaneously functioning with different cards to enter and leave the warehouse. Card readers should be installed in an unreachable distance from each other.

4.2.8. The server room should meet the following requirements along with sub-item 4.2.6. herein:

4.2.8.1. it should be provided with power supply and a generator to ensure uninterrupted electricity.

4.2.8.2. the floor and ceiling of the room should be of antistatic coating.

4.2.8.3. it should be supplied with a thermometer to regulate cooling and heating systems.

4.2.8.4. it should be supplied with humidity meter and regulating equipment.

4.2.9. The area should meet the following requirements along with sub-item 4.2.6. herein for loading and unloading:

4.2.9.1. exchange between a customer and a service center representative should take place only through a window (mechanism) regulated by a dedicated algorithm.

4.2.9.2. all walls should be supplied with seismic detectors to prevent external intrusions.

4.2.9.3. the entrance of the area should be supplied with an intercom to connect to the security room.

4.2.9.4. the entrance door to the area should be supplied with a dedicated card reader and automatically locked, when the window (mechanism) handled with a dedicated algorithm is open.

4.2.10. The room, where PIN-envelopes are printed, should meet the requirements in sub-item 4.2.6. herein and no activities other than PIN-envelopes printing may be carried out there.

4.3. The requirements on handling personnel:

4.3.1. a person responsible for information security should be appointed (the head of the executive authority may not be a responsible person on information security).

4.3.2. the service center should be the primary job of the responsible person on information security.

4.3.3. the staff should have access cards with their first and last names, pictures recognizable with card readers of the rooms they have access to (cards should not reflect any information on the service center).

4.3.4. changes to staff location and changes to access authorities of staff should be documented.

4.3.5. permit for access of a resigned or dismissed employee to systems and the high security zone should be annulled, his/her previously used passwords replaced with new ones without fail.

4.3.6. security service staff should not be authorized to enter the high security zone and personnel's individual data, as well as change the configuration of surveillance cameras, surveillance equipment, motion detectors, fire protection and alarm systems used across the service center.

4.3.7. the staff should be trained at least once a year on rules of behavior in emergency situations and during fire threats and results documented.

4.4. Requirements on creation of interface:

4.4.1. the service center should launch a dedicated exchange of information interface with other service centers on its internal operations.

4.4.2. the service center should create interface for exchange of information with payment and information systems operated by the Central Bank.

5. Oversight and reporting

5.1. The service center shall submit the following documents on the processing activity to the Central Bank for reporting purposes:

5.1.1. written information on managerial bodies and members – in the event of changes to

managerial bodies or the team;

5.1.2. annual financial statements of the service center;

5.1.3. reports of annual audits by international card institutions (if international payment cards are processed);

5.1.4. documents specified in sub-items 3.1.6 – 3.1.8 herein (if changed)

5.1.5. a list of participants using services of the organization – as of 1 April of every year;

5.1.6. written information on offered services and related fee rates - as of 1 April of every year;

5.1.7. information on self-assessment (Annex # 3)

5.1.8. business continuity plan in emergency situations (if changed).

5.2. The service center should submit the documents and data specified in Article 5.1. herein no later than 15 April every year to the Central Bank.

5.3. Emergencies, occurring in the entity (temporary break-up in the system) should be reported to the Central Bank in writing no later than the day following the moment of occurrence.

5.4. The service center should inform the Central Bank in writing 5 (five) days prior to the implementation of the activity specified in sub-item 4.1.13 herein. The report on the result of the activity carried out over the Back-up Center (Annex # 7) should be delivered to the Central Bank within 7 (seven) business days.

5.5. In the event the Central Bank reveals cases of violations of the requirements of these Regulations when analyzing reports, it issues a relevant mandatory instruction for the service center.

6. Termination and revocation of the permit

6.1. The permit issued for the service center may be terminated in the following cases:

6.1.1. at the application of the service center;

6.1.2. if the requirements of Items 5.2, 5.3 and 5.4 herein are violated 2 times in a row;

6.1.3. the service center fails to follow Central Bank's instructions on elimination of violations revealed in the service center performance.

6.2. The Central Bank may revoke the permit, it has issued, in the following cases:

6.2.1. at the application of the service center.

6.2.2. in case of a court order.

6.2.3. if the service center is liquidated.

6.2.4. the case specified in sub-item 6.1.3. herein is not eliminated within the timeframe specified in the administrative act on termination of the permit.

7. Final provisions

7.1. These Regulations shall apply to banks that carry out processing activity, except for Section 3 herein.

7.2. Processing centers that function for a year upon the Regulations become effective should align their processing activity to the requirements of Section 4 herein.

Annex 1
to Regulations on Issue of Permits for and Oversight of the Processing Activity

Questionnaire for the manager of service center's executive body

_____

(name of service center)

1. Personal information

Last name _____

First name _____

Middle name _____

Date and place of birth

_____

Citizenship _____

Marital status _

Address

Military service Yes O No O

Condemnation Yes O No O

Series, number of Personal ID and the name of issuing state authority

2. Education

Name of educational institution	Faculty	Qualification	Period	Series and # of diploma

3. Work experience

Name of entity or organization	Term	Position	Reason for leaving

4. Contact

Contact number(s);

Home Work GSM

Fax (if any); _____

E-mail (if any); _____

Signature

_____

Date

to Regulations on issue of permit for and
oversight of the processing activity

Information on self-assessment

Name of the Service Center _____
Legal address _____
Address, the processing
activity is carried out _____
Phone _____
Fax _____
E-mail _____

Information security (IT systems) security requirements:

Questions	**Yes**	**No**	**Note**
Are high security zone networks, global and local networks separated through network protectors?			
Do all computers have licensed anti-virus software?			
Do all servers have licensed anti-virus software?			
Is there a Back-up Center outside the service center to store systems back-up copies to ensure IT systems' reliable and uninterrupted operations in emergency situations?			

Requirements on security of the area (building) the processing activity will be carried out:

Questions	**Yes**	**No**	**Note**
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Are the surroundings, internal perimeter, entries and exits of the area (building) supplied with surveillance cameras to clearly capture images any time of a day?			
Are all exterior walls, windows, doors and other entrances supplied with seismic, motion or contact detectors to prevent external intrusions?			
Requirements on all entries and exits of the area (building)			
Are entrance doors supplied with card readers which activate the closing mechanism?			
Do entry and exit doors to and from the area (building) open with a special mechanism?			
Are external emergency exits supplied with local alarm signals?			
Are all entries and exits, surroundings of the building (the area) the service center is located in illuminated in the dark time of a day (from sunset to sunrise)?			
Requirements on the control room of the security service			
Are there 2 telephone lines supplied?			
Are there motion detectors supplied?			

Is there an alarm system supplied?			
Is there surveillance equipment supplied?			
Are there hidden buttons for alarm signals?			
Is there a direct communication line between police and fire protection service?			
Is the door equipped with card readers?			
Does only security staff have access?			
Is it located beyond the high security zone?			
If not in the building (area), is it constructed of resilient materials? (stone, brick, concrete)			
Requirements on high security zone:			
Is access to the high security zone equipped with a door or device (lock chamber) opened via a dedicated algorithm (to enter the area if one door is open, the next door should not open and also two separate employees should not be able to enter simultaneously)?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Requirements on personalization rooms:			
Is there a dedicated personalization room?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are doors supplied with alarm signals?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Requirements on the warehouse:			
Is there a dedicated warehouse?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are doors supplied with alarm signals?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			

Is it supplied with internal iron bars?			
To protect from external intrusion, are the floor, ceiling and walls supplied with seismic detectors?			
Requirements on the rooms PIN-envelopes are printed in:			
Is there a dedicated room for PIN-envelopes printing?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are doors supplied with alarm signals?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Requirements on the room where specific waste is stored			
Is there a dedicated room for specific waste?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are doors supplied with alarm signals?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Requirements on the rooms for loading and unloading:			
Is there a dedicated room (area) for loading/unloading?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are doors supplied with alarm signals?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder			

visibility?			
Are all doors supplied with seismic detectors to prevent external intrusions?			
Is the entry to the area supplied with intercom to communicate with the security room?			
Requirements on the server room:			
Is there a dedicated server room?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Is there a power supply for uninterrupted electricity?			
Is there a generator for uninterrupted electricity?			
Is the floor of the room covered with antistatic coating?			
Is the ceiling of the room covered with antistatic coating?			
Is there cooling (air-conditioning) equipment supplied?			
Is a thermometer supplied to regulate heating?			
Is there a humidity meter?			
Is there equipment regulating room's humidity indicators?			

Head of the service center _____
(1st and last named and signature)

Responsible person on Information security _____
(1st and last named and signature)

Date _____
(day/month/year)

Contact numbers _____

Annex #3
to Regulations on issue of permit for and

Information on self-assessment

Name of the Service Center _____
Legal address _____
Address, the processing activity is carried out _____
Phone _____
Fax _____
E-mail _____

Information security (IT systems) security requirements:

Questions	**Yes**	**No**	**Note**
Are external intrusions to the network used for development of personalization data and execution of personalization prevented?			
Are only responsible persons entitled to have access to networks used for development of personalization data and execution of personalization?			
Are personalization files without fail deleted from relevant device's memory upon cards personalization?			
Does the responsible person for information security review and document deletion of personalization files at least quarterly?			
Is the deployment of all hard disks (USB, diskettes, discs) within the high security zone kept under control?			
Are all hard disks (USB, diskettes, disc) used within the high security zone safely stored?			
Are responsible persons for storage and use of all hard disks (USB, diskettes, disc) within the high security zone safely stored designated?			
Is movement of data to and from the high security zone via hard disks by responsible persons registered?			
Is the topological diagram reflecting all system components of the service center adjusted to the current situation?			
Are existing configurations and modifications of network equipment documented?			
Is the internal network of the high security zone, global and local networks separated through network protectors?			
Are parameters of network protectors and related equipment modified by the related responsible person?			
Are all computers protected with licensed anti-virus software?			
Are all servers protected with licensed anti-virus software?			
Is wireless network used to transfer personalization data?			
Are measures taken by the person responsible for			

information security to discover hidden wireless networks and prevent transfer of data through those networks?			
Are penetration tests conducted with the service center no less than once a year or upon changes to network configurations?			
Does the service center have procedures on generation, usage, updating, delivery and cancellation of user passwords in place?			
Is there a Back-up Center to store systems' back-up copies in order to ensure reliable and uninterrupted performance of service center's IT systems in emergency situations?			
Did the service center carry out the processing activity over the Back-up Center to review provision of reliable and uninterrupted performance of service center's IT systems in emergency situations and inform the Central Bank on results?			

Requirements on security of the area (building) the processing activity will be carried out:

Questions	**Yes**	**No**	**Note**
Is the area (building) supplied with fire protection systems, including fire extinguishers?			
Are fire protection systems, including fire extinguishers installed in the area (building) checked for a good condition?			
Are the surroundings, internal perimeter, entries and exits of the area (building) supplied with surveillance cameras to clearly capture images any time of a day?			
Are images of surveillance cameras installed in the surroundings, internal perimeter, entries and exits of the area (building) stored by the security service for at least 6 (six) years?			
Are all exterior walls, windows, doors and other entrances supplied with seismic, motion or contact detectors to prevent external intrusions?			
Requirements on all entries and exits of the area (building)			
Does the security service maintain 24 hour control?			
Is it locked to prevent external intrusion?			
Are entrance doors supplied with card readers which activate the closing mechanism?			
Do entry and exit doors to and from the area (building) open with a special algorithm?			
Are external emergency exits supplied with local alarm signals?			
Are on-door mounted alarm signals checked by the security service monthly and results documented?			
Illuminated boards installed at exits and back-up illuminators checked by the security service monthly and results documented?			

Are all entries and exits, the surrounding of the area (building) in the vicinity of 2 (two) m clearly illuminated in the dark time of the day (from sunset to sunrise)?			
Requirements on the control room of the security service			
Are there 2 telephone lines supplied?			
Are there motion detectors supplied?			
Is there an alarm system supplied?			
Is there surveillance equipment supplied?			
Are there hidden buttons for alarm signals?			
Is there a direct communication line between police and fire protection service?			
Is the door equipped with card readers?			
Does only security staff have access?			
Is it located beyond the high security zone?			
If not in the building (area), is it constructed of resilient materials? (stone, brick, concrete)			
Is the door always locked?			
Does the alarm signal activate if left open for over 30 sec?			
Requirements on high security zone:			
Is access to the high security zone equipped with a door or device (lock chamber) opened via a dedicated algorithm (to enter the area if one door is open, the next door should not open and also two separate employees should not be able to enter simultaneously)?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Requirements on personalization rooms:			
Is there a dedicated personalization room?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Are doors supplied with alarm signals?			
Does the alarm signal activate if left open for over 30 sec?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the door of the room always locked?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			

Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
Requirements on the warehouse:			
Is there a dedicated warehouse?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Are doors supplied with the alarm signal?			
Does the alarm signal activate if left open for over 30 sec?			
Is entry and exit access available with card readers?			
Is the door of the warehouse kept locked?			
Is the area supplied with motion detectors?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Is it supplied with internal iron bars?			
To protect from external intrusion, are the floor, ceiling and walls supplied with seismic detectors?			
Are cards stored in the warehouse inventorized monthly?			
Requirements on the rooms PIN-envelopes are printed in:			
Is there a dedicated room for PIN-envelopes printing?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Are doors supplied with alarm signals?			
Does the alarm signal activate if left open for over 30 sec?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the door of the room always locked?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Do they carry out activities other than PIN-envelopes			

printing?			
Requirements on the room where specific waste is stored			
Is there a dedicated room for specific waste?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Are doors supplied with alarm signals?			
Does the alarm signal activate if left open for over 30 sec?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the door of the room always locked?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Requirements on the rooms for loading and unloading:			
Is there a dedicated room (area) for loading/unloading?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Are doors supplied with alarm signals?			
Does the alarm signal activate if left open for over 30 sec?			
Is entry and exit access available with card readers?			
Is the area supplied with motion detectors?			
Is the door of the room always locked?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
When receiving materials, transfer of PIN-envelopes, ready cards, are all exchanges between customers and representatives of entities made through the window (mechanism) opened with a dedicated algorithm?			
Are all doors supplied with seismic detectors to prevent external intrusions?			

Is the entry to the area supplied with intercom to communicate with the security room?			
Requirements on the server room:			
Is there a dedicated server room?			
Is it supplied with fire-proof furniture?			
Is it constructed of resilient materials? (stone, brick, concrete)?			
Is it supplied with surveillance cameras capable to capture simultaneously the entire area?			
Are images of surveillance cameras capable to capture the entire area stored by the security service for at least 6 (six) years?			
Is the area supplied with alarm signals?			
Does the alarm signal activate if left open for over 30 sec?			
Is entry and exit accessible via in-door mounted card readers?			
Is the area supplied with motion detectors?			
Is the door always locked?			
Is the area (building) supplied with fire protection systems, as well as fire extinguishers?			
Is there an exterior window?			
If yes, is it supplied with iron bars or armored glass?			
If yes, is it covered with films internally to hinder visibility?			
Is there a power supply for uninterrupted electricity?			
Is there a generator for uninterrupted electricity?			
Is the floor of the room covered with antistatic coating?			
Is the ceiling of the room covered with antistatic coating?			
Is there cooling (air-conditioning) equipment supplied?			
Is a thermometer supplied to regulate heating?			
Is there a humidity meter?			
Is there equipment regulating room's humidity indicators?			

Staff requirements:

Questions	**Yes**	**No**	**Note**
Has the head of the service center appointed a responsible person on information security?			
Is the service center the main workplace of the responsible person on information security?			
Does the staff have access cards with their fist and last names, pictures recognizable with card readers of the rooms they have access to?			
Are changes to staff locations and access authorities documented?			
Are permits for access of resigned or dismissed employees to systems and the high security zone annulled, his/her previously used passwords replaced with new ones without fail?			
Is security staff authorized to enter the high security			

zone?			
Does security staff have access to staff's personal data?			
Are security staff members authorized to modify configurations of surveillance cameras, motion detectors, fire protection systems, alarm signals?			
Are staff members regularly trained on how to behave in case of emergency situations and fire threat and results documented?			

Head of the service center _____
(1st and last named and signature)

Responsible person on Information security _____
(1st and last named and signature)

Date _____
(day/month/year)

Contact numbers _____

Annex #4
to Regulations on issue of permit for and

Report on transfer to the Back-up Center

Transfer date and timing	
Execution venue	

Employees involved in organization of transfer to the center:

First and last names	Structural unit	Position

Notes on the work done and final results:_____
_____
_____
_____

Head of the service center _____
(1st and last named and signature)

Responsible person on Information security _____
(1st and last named and signature)

Date _____
(day/month/year)

Contact number _____