**MINISTRY OF INFORMATION SOCIETY AND ADMINISTRATION**

Pursuant to Article 14 paragraph (9) of the Law on Electronic Documents, Electronic Identification and Trust Services (\*) (“Official Gazette of Republic of North Macedonia” no. 101/19 and 275/19), the Minister of Information Society and Administration adopted the following

**RULEBOOK ON THE CONTENT AND THE METHOD OF KEEPING THE REGISTER OF TRUST SERVICE PROVIDERS AND ELECTRONIC IDENTIFICATION SCHEMES, THE METHOD OF SUBMISSION OF THE REQUEST FOR REGISTRATION, THE NECESSARY DOCUMENTATION ENCLOSED TO THE REQUEST, THE REQUEST TEMPLATE AND THE METHOD OF PUBLISHING DATA FROM THE REGISTER**

**Article 1**

The Rulebook herein shall prescribe the content and the method of keeping the Register of trust service providers and electronic identification schemes (hereinafter referred to as: the Register), as well as the method of submission of the request for registration, the necessary documentation enclosed to the request, the request template and the method of publishing data from the register.

**Article 2**

The Register shall contain the following data on the qualified trust service providers:

1) Receipt number of the request for registration in the Register;

2) Name of the qualified trust service provider;

3) Unique Company Identification Number (UCIN);

4) Unique Tax Number (UTN);

5) Seat (street and number, place, postal number and country);

6) Website of the qualified trust service provider;

7) Telephone number and e-mail;

8) Number of the decision on entry in the Register;

9) Date of entry in the Register;

10) Date of establishing of the qualified trust service provider;

11) Registered activity of the qualified trust service provider;

12) Data on the responsible person representing the qualified trust service provider and the scope of authorization:

-  Name and surname;

-  Capacity title;

-  Scope of the authorisations;

-  Telephone number;

-  E-mail;

13) Type of the provisioned qualified trust services;

14) Data on the entry of the change in the Register;

-  Number of the decision on entry of change in the Register;

-  Date of entry of changes in the Register;

15) Data for deletion in the Register:

- Number of the decision on deletion in the Register;

- Date of deletion in the Register.

The Register shall contain the following data on the electronic identification scheme issuers:

Receipt number of the request for registration in the Register;

2)     Name of the electronic identification scheme issuer;

3) Unique Company Identification Number (UCIN);

4) Unique Tax Number (UTN);

5) Seat (street and number, place, postal number and country);

6) Website of the electronic identification scheme issuer;

7) Telephone number and e-mail;

8) Number of the decision on entry in the Register;

9) Date of entry in the Register;

10) Date of establishing the electronic identification scheme issuer;

11) Registered activity of the electronic identification scheme issuer;

12) Data on the responsible person representing the electronic identification scheme issuer and the scope of authorization:

-  Name and surname;

-  Capacity title;

-  Scope of the authorisations;

-  Telephone number;

-  E-mail;

13) Method of proving and verifying the identity of the natural person or the legal entity requesting issuance of electronic identification mean;

14) Means for electronic identification;

15) Method of issuance of the means for electronic identification;

16) Mechanisms for authentication, through which the natural person or the legal entity, by using identification means, validate their identity to the affected party;

17) Security level of the electronic identification scheme;

18) Type of service provisioned by the electronic identification scheme issuer;

19) Data on entry of the change in the Register:

- Number of the decision on entry of change in the Register;

- Date of entry of changes in the Register;

20) Data for deletion in the Register:

- Number of the decision on deletion in the Register;

- Date of deletion in the Register.

The Register shall contain the following data on the non-qualified trust service providers:

1) Receipt number of the request for registration in the Register;

2) Name of the trust service provider;

3) Unique Company Identification Number (UCIN);

4) Unique Tax Number (UTN);

5) Seat (street and number, place, postal number and country);

6) Website of the trust service provider;

7) Telephone number and e-mail;

8) Number of the decision on entry in the Register;

9) Date of entry in the Register;

10) Date of establishing of the trust service provider;

11) Registered activity of the trust service provider;

12) Data on the responsible person representing the trust service provider and the scope of authorization:

-  Name and surname;

-  Capacity title;

-  Scope of the authorisations;

-  Telephone number;

-  E-mail;

13) Type of the provisioned trust services;

14) Data on the entry of the change in the Register;

- Number of the decision on entry of change in the Register;

- Date of entry of changes in the Register;

15) Data for deletion in the Register:

- Number of the decision on deletion in the Register;

- Date of deletion in the Register.

**Article 3**

The Register shall be kept electronically and validated with qualified electronic signature or qualified electronic seal of the Ministry for Information Society and Administration (hereinafter referred to as: the Ministry).

The Register shall be posted on the website of the Ministry.

**Article 4**

The Request for registration of qualified trust service provider in the Register shall be electronically submitted to the Ministry via filled in template enclosed in Annex no. 1 and shall constitute integral part of the Rulebook.

The Request for registration of trust service provider in the Register shall be electronically submitted to the Ministry via filled in template enclosed in Annex no. 2 and shall constitute integral part of the Rulebook.

The Request for registration of electronic identification scheme issuer in the Register shall be electronically submitted to the Ministry via filled in template enclosed in Annex no. 3 and shall constitute integral part of the Rulebook.

The documentation submitted in original or in digital form pursuant to the law shall be enclosed to the requests referred to in paragraphs 1 and 2 of this Article.

The Request can be also submitted in hardcopy to the Ministry archive, while the documentation enclosed to the Request shall be submitted in original or in verified copy.

The entry of the qualified trust service provider and the electronic identification scheme issuer in the Register shall be done on the day of adoption of the decision on entry in the Register.

The templates of the requests for registration referred to in paragraphs 1 and 2 of this Article shall be publicly available on the Ministry website.

**Article 5**

The qualified trust service provider shall enclose the following documentation to the request for registration referred to in Article 4 paragraph 1 of this Rulebook:

1) Insurance policy against professional responsibility for damage and statement for provided funds as a compensation of the damage caused as a result of the provisioning of qualified trust service;

2) Type of the provisioned qualified trust service and the technical standards applied for the provisioning of qualified trust service;

3) General conditions for the provisioning of qualified trust services and information on the qualified trust service provider;

4) Policy for the provisioning of qualified trust services;

5) Statement on conformity with the conditions for performing particular activity;

6) Proof that the necessary technical and organizational measures for risk management were taken which could compromise the security throughout the provisioning of qualified trust service (rulebooks and procedures);

7) Proof that the technical and organizational measures ensure that the security level corresponds to the risk level, considering the latest available technological solutions, and especially taking measures for prevention and reduction of security incidents and limitation of the harmful effects from the potential incidents;

8) Draft contract between the qualified trust service provider and the user thereof;

9) Proof that there is an employee possessing the necessary expertise, experience and qualifications meeting the standards from the area of information security;

10) Certificate for information system security from unauthorized changes and technical security and trust in the supported processes;

11) Certificate for information system security and data preservation;

12) Rules and procedures against forgery, theft and unauthorized access to data;

13) Proof that all relevant information related to data created or received by the qualified trust service provider, especially for providing evidence in court proceedings and for the purpose of ensuring service continuity, are being kept and made available in the corresponding time period, even after the cessation of the activity performance;

14) Proof that the databases are timely, accurate and well protected for issuance of qualified trust certificates if the qualified trust service provider issues certificates;

15) Bylaws from the area of personal data protection in accordance with the Law on Personal Data Protection;

16) Procedures used by the qualified trust service provider for the provisioning of the services;

17) Report on the assessment of the conformity prepared by the conformity assessment body;

18) Plan for the cessation of activity.

Apart from the documentation referred to in paragraph 1 of this Article, the qualified trust service providers using the loyalty mark for the qualified trust service for which they were registered should also submit a statement that the loyalty mark shall be linked to the list of qualified trust service providers and qualified trust services.

The qualified trust service providers who shall issue qualified electronic signature or qualified electronic seal, apart from the documentation referred to in paragraph 1 of this Article, should also submit a report on the assessment of the conformity of the means for issuing qualified electronic signature or qualified electronic seal, prepared by accredited laboratory for testing of the means.

**Article 6**

The non-qualified trust service provider shall enclose the following documentation to the request referred to in Article 4 paragraph 2 of this Rulebook:

1) Insurance policy against professional responsibility for damage and statement for provided funds as a compensation of the damage caused as a result of the provisioning of trust service;

2) Type of the provisioned trust service and the technical standards applied for the provisioning of trust service;

3) General conditions for the provisioning of trust services and information on the trust service provider;

4) Policy for the provisioning of trust services;

5) Statement on conformity with the conditions for performing particular activity;

6) Proof that the necessary technical and organizational measures for risk management were taken which could compromise the security throughout the provisioning of trust services (rulebooks and procedures).

**Article 7**

The electronic identification scheme issuer shall enclose the following documentation to the request referred to in Article 4 paragraph 3 of this Rulebook:

1) Statement on the provisioned funds for compensation of the damage caused by the use of electronic identification schemes;

2) Method of proving and verifying the identity of the natural person or the legal entity requesting issuance of electronic identification mean;

3) Procedure for the method of issuance of the means for electronic identification;

4) Mechanisms for authentication, through which the natural person or the legal entity, by using identification means, validate their identity to the affected party;

5) Conditions that should be met by the other participants included in the procedure for issuing means for electronic identification;

6) Description of the technical and security features of the means for electronic identification issued within the scheme;

7) Technical and organizational measures met by the issuer of electronic identification means for the purpose of ensuring interoperability of the electronic identification schemes in accordance with the national and international standards in this area;

8) Report on the security level of the electronic identification scheme by the compliance assessment body;

9) Rulebooks or procedures for technical, physical and organizational measures corresponding to the risk level and the planned security level of the electronic identification scheme;

10) Rulebook on determining the conditions and standards which should be met by the technical and organizational measures for security of electronic identification schemes containing measures for prevention of security incidents and for limitation of the harmful effects from the potential incidents;

12) Certificate for information system security from unauthorized changes and technical security and trust in the supported processes;

13) Certificate for information system security and data preservation;

14) Rules and procedures against forgery, theft and unauthorized access to data;

15) Proof of keeping and making available all relevant information related with the data created or received by the electronic identification scheme issuer, within particular time period, even after the cessation with the performance of the activity, especially for providing evidence in court proceedings and for the purpose of ensuring continuity of the service;

16) Bylaws from the area of personal data protection in accordance with the Law on Personal Data Protection;

17) Report on the assessment of the compliance prepared by compliance assessment body;

18) Plan for the cessation of activity; and

19) Report on the assessment of the compliance of the means for electronic identification, prepared by the accredited laboratory for testing means.

**Article 8**

The qualified trust service provider or the qualified trust service provided by the provider i.e. the issuer of electronic identification schemes in the event of change of the circumstances affecting the data being entered in the Register or the proof enclosed to the request for registration shall submit a request to the Ministry for change of data in the Register within seven days as of the day of the change.

In the event of change of data at the non-qualified trust service provider or the non-qualified trust service provided by the provider, the non-qualified trust service provider shall submit a request to the Ministry for change of data in the Register within seven days as of the day of the change.

The change of data entered in the Register shall be done in the same method as the registration in the Register by enclosing the relevant documentation referring to the change as an Annex to the Request.

**Article 9**

Notwithstanding the provisions referred to in Articles 5, 6, 7 and 8 of this Rulebook, foreign legal entities registered as trust service providers or as electronic identification scheme issuers on EU level or in EU member state, as well as foreign legal entities registered as trust service providers or as electronic identification scheme issuers in a country which is not EU member state, based on previously concluded contract regulating the reciprocity of the electronic identification schemes and/or trust service providers between Republic of North Macedonia and the country where the legal entity is registered, shall be entered in the Register by taking data from the list on EU level or the member state or the country where they are registered.

**Article 10**

The Rulebook herein shall enter into force on the next day as of the day of publishing thereof in the “Official Gazette of the Republic of North Macedonia”.

|  |  |
| --- | --- |
| No. 11/1-1069/3 | Minister of Information |
| 14 February 2020 | Society and Administration |
| Skopje | **Damjan Mancevski** |

Annex no. 1

Request

for registration of qualified trust service provider in the Register of

qualified trust service providers and electronic identification schemes

|  |  |  |
| --- | --- | --- |
| Data on the request submitter | | |
| Name of the legal entity |  | |
| UCIN |  | |
| UTN |  | |
| Seat | Street and number |  |
| Postal number |  |
| Place |  |
| Country |  |
| Website |  | |
| E-mail |  | |
| Telephone |  | |
| Data on the entry of the request submitter in the trade register and in the register of  other legal entities in accordance with the Law on One-Stops Shop System | | |
| Register title |  | |
| Number of the decision on entry in the register |  | |
| Date of entry |  | |
| Organizational form |  | |
| Activity code |  | |
| Activity description |  | |
| Responsible persons for submission of the request | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
|  | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
|  | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
| Data for which change is being requested\* | | |
| Datum type | Current datum | New datum |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\*The part referring to data for which change is being requested shall be filled in only if change is being required of data which are already entered in the Register.

|  |  |
| --- | --- |
| Necessary documentation for the qualified trust service provider\* | |
| 1) Insurance policy against professional responsibility for damage and statement for provided funds as a compensation of the damage caused as a result of the provisioning of qualified trust service | □ |
| 2) Type of the provisioned qualified trust service and the technical standards applied for the provisioning of qualified trust service | □ |
| 3) General conditions for the provisioning of qualified trust services and information on the qualified trust service provider | □ |
| 4) Policy for the provisioning of qualified trust services | □ |
| 5) Statement on compliance with the conditions for performing particular activity | □ |
| 6) Proof that the necessary technical and organizational measures for risk management were taken which could compromise the security throughout the provisioning of qualified trust service (rulebooks and procedures) | □ |
| 7) Proof that the technical and organizational measures ensure that the security level corresponds to the risk level, considering the latest available technological solutions, and especially taking measures for prevention and reduction of security incidents and limitation of the harmful effects from the potential incidents | □ |
| 8) Draft contract between the qualified trust service provider and the user thereof | □ |
| 9) Proof that there is an employee possessing the necessary expertise, experience and qualifications meeting the standards from the area of information security | □ |
| 10) Certificate for information system security from unauthorized changes and technical security and trust in the supported processes | □ |
| 11) Certificate for information system security and data preservation | □ |
| 12) Rules and procedures against forgery, theft and unauthorized access to data | □ |
| 13) Proof that all relevant information related to data created or received by the qualified trust service provider, especially for providing evidence in court proceedings and for the purpose of ensuring service continuity, are being kept and made available in the corresponding time period, even after the cessation of the activity performance | □ |
| 14) Proof that the databases are timely, accurate and well protected for issuance of qualified trust certificates if the qualified trust service provider issues certificates | □ |
| 15) Bylaws from the area of personal data protection in accordance with the Law on Personal Data Protection | □ |
| 16) Procedures used by the qualified trust service provider for the provisioning of the services | □ |
| 17) Report on the assessment of the compliance prepared by compliance assessment body | □ |
| 18) Plan for the cessation of activity | □ |
| 19) Statement that the qualified trust service provider shall link the loyalty mark for which it is registered with the list of qualified trust service providers of the qualified trust service provider intends to use the loyalty mark | □ |
| 20) Report on the assessment of the compliance of the means for issuance of qualified electronic signatures or qualified electronic seals, prepared by the accredited laboratory for testing means of the qualified trust service provider who shall issue qualified electronic signature or qualified electronic seal | □ |

\* If change of data entered in the Register is required, only the documentation referring to such data shall be submitted.

Annex no. 2

Request

for registration of trust service provider in the Register of

trust service providers and electronic identification schemes

|  |  |  |
| --- | --- | --- |
| Data on the request submitter | | |
| Name of the legal entity |  | |
| UCIN |  | |
| UTN |  | |
| Seat | Street and number |  |
| Postal number |  |
| Place |  |
| Country |  |
| Website |  | |
| E-mail |  | |
| Telephone |  | |
| Data on the entry of the request submitter in the trade register and in the register of  other legal entities in accordance with the Law on One-Stops Shop System | | |
| Register title |  | |
| Number of the decision on entry in the register |  | |
| Date of entry |  | |
| Organizational form |  | |
| Activity code |  | |
| Activity description |  | |
| Responsible persons for submission of the request | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
|  | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
|  | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
| Data for which change is being requested\* | | |
| Datum type | Current datum | New datum |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\*The part referring to data for which change is being requested shall be filled in only if change is being required of data which are already entered in the Register.

|  |  |
| --- | --- |
| Necessary documentation for the trust service provider\* | |
| 1) Insurance policy against professional responsibility for damage and statement for provided funds as a compensation of the damage caused as a result of the provisioning of qualified trust service | □ |
| 2) Type of the provisioned qualified trust service and the technical standards applied for the provisioning of qualified trust service | □ |
| 3) General conditions for the provisioning of trust services and information on the trust service provider | □ |
| 4) Policy for the provisioning of trust services | □ |
| 5) Statement on compliance with the conditions for performing particular activity | □ |
| 6) Proof that the necessary technical and organizational measures for risk management were taken which could compromise the security throughout the provisioning of trust services (rulebooks and procedures) | □ |

\* If change of data entered in the Register is required, only the documentation referring to such data shall be submitted.

Annex no. 3

Request

for registration of electronic identification scheme issuer in the Register of

trust service providers and electronic documentation schemes

|  |  |  |
| --- | --- | --- |
| Data on the request submitter | | |
| Name of the electronic identification scheme issuer |  | |
| UCIN |  | |
| UTN |  | |
| Seat | Street and number |  |
| Postal number |  |
| Place |  |
| Country |  |
| Website |  | |
| E-mail |  | |
| Telephone |  | |
| Data on the entry of the request submitter in the trade register and in the register of  other legal entities in accordance with the Law on One-Stops Shop System | | |
| Register title |  | |
| Number of the decision on entry in the register |  | |
| Date of entry |  | |
| Organizational form |  | |
| Activity code |  | |
| Activity description |  | |
| Responsible persons for submission of the request | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
|  | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
|  | | |
| Name and surname |  | |
| Capacity title |  | |
| Scope of authorizations |  | |
| Telephone |  | |
| E-mail |  | |
| Data on the person managing the procedure for registration of  unique data on identification of persons | | |
| Name of the person managing the procedure for registration of unique data on identification of the persons |  | |
| PIN |  | |
| UTN |  | |
| Seat | Street and number |  |
| Postal number |  |
| Place |  |
| Country |  |
| Website |  | |
| E-mail |  | |
| Telephone |  | |
| Data on the entity conducting the authentication procedure | | |
| Name of the entity conducting the authentication procedure |  | |
| UCIN |  | |
| UTN |  | |
| Seat | Street and number |  |
| Postal number |  |
| Place |  |
| Country |  |
| Website |  | |
| E-mail |  | |
| Telephone |  | |
| Data on the compliance assessment body | | |
| Name of the compliance assessment body |  | |
| UCIN |  | |
| UTN |  | |
| Seat | Street and number |  |
| Postal number |  |
| Place |  |
| Country |  |
| Website |  | |
| E-mail |  | |
| Telephone |  | |
| Data on the electronic identification scheme | | |
| Name of the electronic identification scheme |  | |
| Scheme security level(s) |  | |
| Description of the electronic identification scheme (including short description of the scheme, context of operation, scope, additional attributes which may be given for natural persons and legal entities within the scheme at the request of the affected party) |  | |
| Description of the scheme supervision method (including information on the roles, responsibilities and authorizations of the supervisory body and the issuer of the scheme, method of supervising the issuer and the entity conducting the authentication procedure) |  | |
| Applicable procedures for scheme management (suspension or confiscation of the entire scheme or compromised parts thereof) |  | |
| Method of entry in the scheme (including data on signing on and registration, certificate for identity verification and connection of the means for electronic identification of natural persons and legal entities) |  | |
| Features and design of the means for electronic identification (including data on security certification, if any) |  | |
| Issuance, delivery and activation of the scheme |  | |
| Suspension, revocation and reactivation of the scheme |  | |
| Renewal and replacement of the scheme |  | |
| Procedure for scheme authentication |  | |
| Scheme management and organization (including general data on management and organization, published notices and data on the user, information security management, recording records, facilities and human resources, technical controls, compliance and audit) |  | |
| Description of the implementation level of the standards and minimum technical and security conditions for interoperability |  | |
| Data for which change is being requested\* | | |
| Datum type | Current datum | New datum |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\*The part referring to data for which change is being requested shall be filled in only if change is being required of data which are already entered in the Register.

|  |  |
| --- | --- |
| Necessary documentation for the electronic identification scheme issuer\* | |
| 1) Statement on the provisioned funds for compensation of the damage caused by the use of electronic identification schemes | □ |
| 2) Procedure on the method of proving and verifying the identity of the natural person or the legal entity requesting issuance of the mean for electronic identification | □ |
| 3) Procedure on the method of issuing means for electronic identification | □ |
| 4) Description of the mechanisms for authentication, through which the natural person or legal entity, by using the means of identification, validate the identity of the affected party | □ |
| 5) Conditions that should be met by the other participants included in the procedure for issuing means for electronic identification | □ |
| 6) Description of the technical and security features of the means for electronic identification issued within the scheme | □ |
| 7) Technical and organizational measures met by the issuer of electronic identification means for the purpose of ensuring interoperability of the electronic identification schemes in accordance with the national and international standards in this area | □ |
| 8) Report on the security level of the electronic identification scheme by the compliance assessment body | □ |
| 9) Rulebooks or procedures for technical, physical and organizational measures corresponding to the risk level and the planned security level of the electronic identification scheme | □ |
| 10) Rulebook on determining the conditions and standards which should be met by the technical and organizational measures for security of electronic identification schemes containing measures for prevention of security incidents and for limitation of the harmful effects from the potential incidents | □ |
| 11) Proof that there is an employee possessing the necessary expertise, experience and qualifications for application of information system security | □ |
| 12) Certificate for information system security from unauthorized changes and technical security and trust in the supported processes | □ |
| 13) Certificate for information system security and data preservation | □ |
| 14) Rules and procedures against forgery, theft and unauthorized access to data | □ |
| 15) Proof of keeping and making available all relevant information related with the data created or received by the electronic identification scheme issuer, within particular time period, even after the cessation with the performance of the activity, especially for providing evidence in court proceedings and for the purpose of ensuring continuity of the service | □ |
| 16) Bylaws from the area of personal data protection in accordance with the Law on Personal Data Protection | □ |
| 17) Report on the assessment of the compliance prepared by the compliance assessment body | □ |
| 18) Plan for the cessation of activity | □ |
| 19) Report on the assessment of the conformity of the means for electronic identification, prepared by the accredited laboratory for testing means | □ |

\* If change of data entered in the Register is required, only the documentation referring to such data shall be submitted.