Pannon Egyetem
University of Pannonia

REGULATION ON THE USE OF ELECTRONIC SIGNATURES AND ELECTRONIC STAMPS

Adopted by the Senate on:	**27th November 2025**
Senate Resolution Number:	**199/2025. (XI.27.)**
Effective date:	**1st January 2026**
Person responsible for the maintenance of this Regulation:	**Head of the Directorate of Information Technology**
Version number: 00	

version number	date of publication	effective date	date of repeal	Senate Resolution No., Board of Trustees Resolution No.*
00	05.01.2026	01.01.2026	-	199/2025. (XI.27.)

*if entry into force of the Regulation is subject to adoption by the Board of Trustees

Table of Contents

Chapter I **4**
GENERAL PROVISIONS **4**
1.§ 4
Purpose of the Regulation 4
2.§ 4
Scope of the Regulation, applicable legislation and rules 4
3.§ 5
Definitions 5
4.§ 8
Persons authorised to use electronic signatures and electronic stamps 8
5. § 8
Scope of application of electronic signatures and electronic stamps 8
Chapter II **9**
RULES FOR THE USE OF ELECTRONIC SIGNATURES AND ELECTRONIC STAMPS **9**
6. § 9
Requesting and receiving electronic signature and electronic stamp services and related responsibilities 9
7.§ 11
Application of electronic signatures and electronic stamps 11
8.§ 11
Rules for the use of signature creation devices 11
9.§ 12
Common rules on the validity of electronic signatures and electronic stamps 12
10.§ 13
Rules for the management of signature certificates used on behalf of the University 13
11.§ 15
Long-term preservation (archiving) and counter-authentication of documents bearing electronic signatures and electronic stamps 15
Chapter III **15**
FINAL PROVISIONS **15**
12.§ 15

The Regulation on the Use of Electronic Signatures and Electronic Stamps (hereinafter referred to as the "**Regulation**") issued by the University of Pannonia (hereinafter referred to as the "**University**") on the basis of the Organisational and Operational Rules (hereinafter referred to as the "**OOR**"), Part I Organisational and Operational Rules of Procedure (hereinafter referred to as the "**OORP**") approved by the Senate of the University of Pannonia and adopted by the Foundation for the University of Pannonia acting as the operator exercising founders' and ownership rights (hereinafter referred to as the "**Operator**") and on the basis of the resolution by the Board of Trustees on the rules of procedure for adopting the regulations of the University of Pannonia by the Board of Trustees is as follows.

Chapter I

GENERAL PROVISIONS

1.§

Purpose of the Regulation

(1) The purpose of this Regulation is to define the procedures for the creation, use and verification of electronic signatures and electronic stamps applied at the University, as well as the related authorisations, technological solutions and the rules for handling documents bearing electronic signatures and/or electronic stamps.

2.§

Scope of the Regulation, applicable legislation and rules

(1) The personal scope of this Regulation shall extend to all faculties, comprehensive organisational units and organisational units of the University (hereinafter collectively referred to as '**organisational units**'), as well as to all individuals employed by the University or engaged in any other work-related

legal relationship, who are authorised to sign documents in accordance with the University's regulations, or who participate in the administrative handling of electronically signed documents.

(2) The material scope of this Regulation shall extend to the electronic signing and affixing of electronic stamps on documents created in electronic form by persons authorised to sign within the scope of their authority, to the electronic signature and electronic stamp solutions applicable at the University, to the rules for verifying electronically signed or electronically stamped documents, to the transmission of documents bearing an electronic signature or electronic stamp by the University via the Government Gateway or other electronic means, to the storage and re-authentication of electronic documents bearing an electronic signature or electronic stamp, and to the requesting, use and destruction of electronic signature creation devices.

(3) Legislation and regulations applied in the preparation of this Regulation:

a. Regulation (EU) 910/2014 of the European Parliament and of the Council (eIDAS);
b. Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services;
c. Information Technology Regulation of the University of Pannonia;
d. Document Management Regulation of the University of Pannonia;
e. Contracting Policy of the University of Pannonia;
f. Organisational and Operational Rules of the University of Pannonia – Part II: Employment Requirement System;
g. Regulation of Powers and Competence Relating to Financial Management.

3.§

Definitions

(1) **Signature creation data:** unique data (typically a cryptographic private key) used by the signatory to create an electronic signature.

(2) **Signature creation device:** hardware or software used by the signatory to create an electronic signature using signature creation data.

(3) **Signatory:** a natural person authorised to sign documents who is entitled to sign the generated document with their handwritten signature and who, in possession of a signature creation device, is authorised to sign pursuant to

Section 4(2) of this Regulation and places the electronic signature on the electronic document.

(4) **Signature verifier:** the person or supervised signing automation that receives the signed electronic document and verifies the integrity of the message by comparing the content of the electronically signed message at the time of signing and at the time of verification, and identifies the signatory using the message, the signature verification data published by the trust service provider, certificate revocation information and the certificate.

(5) **Electronic signature:** electronic data logically associated with or inseparably linked to an electronic document for the purpose of identifying the signatory, created using the signatory's private key and proving beyond doubt the origin, authenticity and integrity of the document as well as the fact of signature, which can be verified exclusively by means of the corresponding public key.

(6) **Electronic document:** a set of data that can be interpreted by electronic means.

(7) **Electronic stamp:** an electronic signature used by the University to identify itself.

(8) **Qualified electronic stamp:** an advanced electronic stamp created using a qualified electronic stamp creation device and based on a qualified certificate for electronic stamps (Article 3 of the eIDAS Regulation).

(9) **Creator of an electronic stamp:** the legal person that creates an electronic stamp.

(10) **User:** a person signing an electronic document, a party verifying a signature or a device or application that uses keys, certificates and timestamps issued within the scope of the services for their intended purpose.

(11) **Advanced electronic signature:** an electronic signature that meets the requirements set out in Article 26 of the eIDAS Regulation, namely that it:

a. is uniquely linked to the signatory;
b. is capable of identifying the signatory;
c. is created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control;
d. is linked to the signed data in such a way that any subsequent change in the data is detectable.

(12) **Trust service provider / Provider:** a natural or legal person who, within the framework of trust services, identifies the person requesting a certificate, issues a certificate to them (which may relate to the applicant, the University

or the organisational unit associated with the applicant), maintains registers, receives data concerning changes related to certificates, and publishes the policies related to the certificate, signature verification data and information regarding the current status of the certificate (in particular its possible revocation).

(13) **Timestamping:** the process by which an electronic document is provided with proof (an electronic timestamp) containing the authenticated time of timestamping and linked to the document in such a way that any modification after the issuance of the proof is detectable.

(14) **Electronic timestamp:** a set of electronic data attached to or logically associated with other electronic data for the purpose of ensuring the origin and integrity of the linked data and reliably proving the exact time of signing and that the electronic document already existed in unchanged form at the time of timestamping.

(15) **Timestamp service provider:** a service provider with an authenticated and highly accurate time source that issues timestamps to subscribers requesting them and attaches them to electronically signed electronic documents or their hashes.

(16) **Requestor of a personal electronic signature certificate:** a user employed by the University whose duties require the use of an electronic signature certificate and signature creation device, particularly managers authorised to sign documents and exercising delegated authority for financial commitments.

(17) **Requestor of an institutional electronic stamp:** a user employed by the University whose duties require the use of an institutional electronic stamp.

(18) **Qualified electronic signature:** an advanced electronic signature created using a qualified electronic signature creation device and based on a qualified certificate for electronic signatures. It provides the highest level of security, has the same legal effect as a handwritten signature and creates a private document with full probative value.

(19) **Certificate:** an electronic signature certificate, an electronic stamp certificate or any other electronic attestation issued by the service provider within the framework of trust services containing validation data relating to the certificate and associated data necessary for its use, which is reliably protected against forgery using the technologies available at the time of issuance and throughout its validity period.

(20) **Partner:** any natural person or legal person, or organisation without legal personality to whom the University transmits, or from whom it receives electronically created and electronically signed documents in the course of procedures falling within its competence.

4.§

Persons authorised to use electronic signatures and electronic stamps

(1) Among the employees of the University, the right to sign shall be exercised by the persons specified in the University's Deed of Foundation and Organisational and Operational Rules of Procedure, as well as by persons authorised to sign under powers delegated by the Rector or the Chancellor in accordance with the University's Regulation of Powers and Competence Relating to Financial Management, and by persons authorised by the Rector or the Chancellor with regard to the use of the electronic stamp.

(2) At the University, the following persons are authorised to use advanced and/or qualified electronic signatures:

   a. employees holding managerial positions as defined by the Employment Requirement System;
   b. employees authorised to undertake financial commitment or to provide financial countersignature;
   c. persons who, pursuant to legal provisions or the internal regulations of the University, may fulfil their obligations exclusively by means of electronically authenticated documents.

(3) The Service Provider shall generate and, following personal identification, provide the authorised employee with the signing certificate and the device necessary for the creation of an electronic signature.

5. §

Scope of application of electronic signatures and electronic stamps

(1) Electronic signatures may be used for the following types of documents:

   a. contracts concluded with external partners (provided that the contracting partner possesses a certified electronic signature);
   b. application and tender documents;
   c. official documents;

d. any other documents required by law.

(2) Electronic signatures shall not be applicable in the following cases:

a. personal employment-related documents regulated by Act I of 2012 on the Labour Code (e.g. employment contracts, job descriptions, etc.);
b. documents for which legislation expressly requires a paper-based format;
c. contracts concluded with external partners if the contracting partner does not possess a qualified electronic signature.

(3) Electronic stamps may be used for the following types of documents:

a. documents authorised by the Rector, the Chancellor or managers vested with delegated authority by them.

(4) Documents created by the University in electronic form and bearing an electronic signature or electronic stamp shall be transmitted to recipients not listed in the Public Service e-Address Register via the official electronic gateway, provided the recipient has an official gateway/company gateway/client gateway, or by other electronic means. In the case of documents generated in the Unified Educational System, transmission shall take place through the Neptun system, in compliance with the provisions of the Document Management Regulation, the Information Technology Regulation and the Privacy and Data Protection Policy.

Chapter II

RULES FOR THE USE OF ELECTRONIC SIGNATURES AND ELECTRONIC STAMPS

6. §

Requesting and receiving electronic signature and electronic stamp services and related responsibilities

(1) Signature creation data (keys) and signature or stamp certificates may only be requested in accordance with the provisions set out in the Procurement

Policy of the University of Pannonia, through a procurement procedure and on the basis of a service contract concluded with the Service Provider selected during the procedure (hereinafter referred to as the '**Contract**'). The procurement request submitted within the procedure must indicate the approval of the Chancellor.

(2) The verification of the signing authority of a University employee authorised to use an electronic signature shall be carried out by means of a declaration made in the form required by the Service Provider.

(3) The Service Provider shall generate and, following personal identification, provide the authorised employee with the signing certificate and the device required to create the electronic signature. The employee shall report this to his or her **supervisor**, whose related responsibilities include the following:

a. notifying the Directorate of Human Resources Management (hereinafter referred to as '**DHRM**') so that the signature creation device and the certificate are recorded as being issued for the employee's personal use in accordance with the relevant Chancellor's Directive and the provisions of the Inventory Control and Inventory Preparation Policy of the University of Pannonia;

b. notifying the University's Directorate of Economic Affairs in order for the device and certificate to be entered into the inventory.

(4) The public data of the certificates issued and used for electronic signatures and electronic stamps, as well as the name of the authorised recipient, shall be recorded in the register maintained by the **Directorate of Information Technology** (hereinafter referred to as '**DIT'**). In the case of electronic stamp certificates, the register shall also include the method and purpose of the certificate's use.

(5) The **DHRM** shall maintain an up-to-date register in the Nexon HR administration system regarding the assignment of signature creation devices and certificates to employees and shall track any changes therein. In the event of a change in signing authorisation, the employee concerned shall immediately notify his or her supervisor and the Director of the DIT, who shall request the User to report the change to the Service Provider. Tasks related to electronic stamps shall be performed by the DIT.

(6) Within the scope of its responsibilities, the **Service Provider** shall receive and process data changes reported by the Requestor throughout the entire lifecycle of the signature and stamp certificates issued to the employee using the service, accept and process renewal requests, and, where necessary, suspend or revoke the certificate.

7.§

Application of electronic signatures and electronic stamps

(1) In connection with the performance of the tasks specified in its Deed of Foundation, the University shall create and register documents in electronic form or generate electronic documents from paper-based records and shall authenticate them with an electronic signature and timestamp or with an electronic stamp and timestamp.
(2) Document authentication using an electronic stamp shall be carried out using at least an advanced electronic signature certificate.
(3) Authentication of electronic documents using an electronic signature shall be carried out using a qualified electronic signature certificate.
(4) If identification of the signatory is not required (e.g. in the case of diplomas), authentication of electronic documents shall be performed using an electronic stamp.
(5) The electronic signature used by employees of the University authorised to sign documents, as well as its graphical representation, shall contain at least:
    a. the full name of the person creating the electronic signature as stated in their personal identification document,
    b. the position of the person creating the electronic signature in the case of electronic signatures applied to documents managed by the University, as provided for in Article 34 of Government Decree 87/2015 (IV.9.),
    c. the date and exact time of the signature,
    d. in the case of a chamber legal counsel, the chamber identification number (CIN).

8.§

Rules for the use of signature creation devices

(1) A person authorised to sign documents, using a smart chip card or token and the corresponding password, may:
    a. create a qualified electronic signature or apply an electronic stamp to an electronic document using software provided by the Service Provider within the IT system or introduced by the University for signing purposes; or

b. apply a counter-authentication to a previously created electronic document using an electronic signature and a qualified timestamp.

(2) An employee authorised to use an electronic signature or electronic stamp may exercise this authorisation only in the course of administrative procedures falling within the competence of the University and while acting on behalf of the University. The electronic signature may not be used for private purposes or for matters outside the scope of signing authority.

(3) An employee authorised to use an electronic signature or electronic stamp shall store the signature creation device issued to them in a secure location, separately from the PIN (e.g. in a locked drawer, cabinet or file cabinet).

(4) In the event of loss or compromise of the electronic data carrier or the associated password, or if the password is lost or forgotten, the employee concerned shall immediately notify his or her superior, the Director of the DIT, the University's data protection contact person and the Service Provider, and simultaneously request the suspension of the certificate.

(5) A person authorised to use an electronic signature or electronic stamp may not transfer the electronic signing device or the envelopes containing the PIN required for its use to another person, even temporarily. These devices and codes are non-transferable.

9.§

Common rules on the validity of electronic signatures and electronic stamps

(1) During the verification of the authenticity of a document electronically signed by a Partner, the following aspects shall be examined:

a. the identity of the signatory,
b. the validity of the signature, and
c. the presence of the timestamp embedded in the signature.

(2) The electronic signature, the electronic stamp and the certificates associated with them shall be verified. The authenticity of the signatures of electronic documents stored in the document management system shall be verified using appropriate application software designed for this purpose.

(3) An electronic signature and/or electronic stamp shall not be accepted if any data contained in the signature certificate or in any certificate within the validity chain indicates that the signature and/or stamp is invalid, or if the authenticity verification performed pursuant to Section (2) herein results in findings indicating the invalidity of any of the above.

(4) A timestamp shall not be accepted if the certificate of the electronic signature or electronic stamp used for timestamping or any certificate in the validity chain, contains data indicating that it is invalid.

(5) Following the receipt of a document bearing an electronic signature, the head of the organisational unit professionally responsible for the case concerned or an employee authorised by them shall be responsible for verifying the electronic signature on the electronically received document by examining the validity chain.

10.§

Rules for the management of signature certificates used on behalf of the University

(1) If

a. the signature creation device or the password required for its use is lost by the person possessing the electronic signature,
b. the signature creation device or the password required for its use is stolen,
c. the signature creation device or the password required for its use becomes publicly known, or
d. there is suspicion that any of the events listed in paragraphs a) to c) has occurred,

the User shall immediately initiate a suspension procedure with the Service Provider in accordance with the method specified in the Contract.

(2) In the cases set out in Section (1) herein, the User may request the termination of the suspension of the certificate and the restoration of its validity from the Service Provider in accordance with the procedure specified in the Contract. The User shall inform his or her supervisor and the Director of the DIT in writing of any change in the certificate status no later than the working day following the event affecting the certificate status. In the cases referred to in paragraphs a) to c) of Section (1), the University's data protection contact person shall also be notified.

(3) If any of the events specified in Section (1) herein occurs and is not resolved within the time limit specified in the Contract, the User shall officially initiate a certificate revocation procedure with the Service Provider. If the Service Provider does not receive notification that the compromising event has been resolved, the certificate shall be invalidated on the date specified in the Contract.

(4) The User shall notify the Director of the DIT if any change occurs in their name, personal data or position that affects their signing authorisation. The Director of the DIT shall request the User to report the change to the Service Provider. Where necessary, the Director of the DIT is authorised to notify the Service Provider of changes affecting signing authorisation on their own authority.

(5) The User shall notify the Service Provider and the Director of the DIT of any change in the organisational data recorded in the certificate issued for the electronic signature used by the University.

(6) If signing authorisation ceases due to termination of employment, change of organisational unit or position, at the request of the authorised employee, or for any other reason, the User shall notify the Director of the DIT and simultaneously initiate the revocation of the signature creation device with the Service Provider without delay, as well as request the withdrawal of the device issued for personal use through their supervisor. Upon revocation, the certificate shall permanently lose its validity, and any electronic signature created on the basis of the revoked certificate shall no longer be suitable for document authentication. The procedure for termination is specified in the agreement concluded between the University and the Service Provider.

(7) In connection with the revocation of the signature creation device, the Director of the DIT and the DHRM shall ensure that the relevant registers are updated.

(8) Following the revocation of the signature creation device, the device shall be handed over to the staff of the DIT, who shall render it unsuitable for signing and draw up a written record of this action.

(9) The record shall include the unique identification number of the signature creation device rendered unsuitable for signing, the fact and date of the change of status and the signatures of the persons present at the time of the status change and of the Director of the DIT.

(10) The change of status shall be carried out in such a way that the signature creation device can no longer be used to create electronic signatures.

(11) The User shall notify the Service Provider and the Director of the DIT of any change in the organisational data recorded in the certificate issued for the electronic signature and/or electronic stamp used by the University.

11.§

Long-term preservation (archiving) and counter-authentication of documents bearing electronic signatures and electronic stamps

(1) The purposes of archiving are:
   a. to protect the confidentiality and integrity of documents,
   b. to prevent unauthorised access,
   c. to exclude the possibility of subsequent modification.

(2) With regard to documents created and authenticated with an electronic signature or electronic stamp, the University shall ensure that, until the expiry of the retention period specified in Annex 3 to the Document Management Regulation, the Unified Records Retention Schedule of the University of Pannonia, documents created or received in the course of the University's administrative processes and authenticated with an electronic signature or electronic stamp remain interpretable (readable) and retrievable, and are accessible in an unchanged form corresponding to their state at the time of signature.

(3) Concerning the counter-authentication of electronic documents, the University shall ensure, through the Director of the DIT, the conclusion of an appropriate contract with the Service Provider responsible for counter-authentication, in accordance with the provisions set out in the Procurement Policy of the University of Pannonia.

(4) The DIT shall maintain a register of the validity periods of qualified certificates provided by the respective Service Providers and shall notify the User at least two months before their expiry in order to initiate the procurement procedure for obtaining a new certificate in accordance with the provisions of the Procurement Policy of the University of Pannonia.

Chapter III

FINAL PROVISIONS

12.§

(1) This Regulation shall be promulgated and published by the University on its website (www.uni-pannon.hu).
(2) This Regulation shall enter into force on 1st January 2026.
(3) This Regulation was adopted by the Senate at its meeting held on 27th November 2025 by Resolution No. 199/2025. (XI.27.).
(4) This Regulation shall remain in force until withdrawn.

Date in Veszprém, on 27th November 2025

Dr. János Abonyi Rector	Zsolt Csillag Chancellor

Approved on behalf of the Foundation for the University of Pannonia, acting as the maintaining body:

Dated in Veszprém, on 27th November 2025

Dr. Péter Bartus

Executive Director