

REGULATION

on the Use of Artificial Intelligence Systems by the Supreme Court Staff

Section I. General Provisions

1. Subject Matter and Scope of the Regulation

1.1. This Regulation lays down the rules governing the use of artificial intelligence systems by employees of the Supreme Court Staff in the performance of their official duties.

1.2. This Regulation applies to civil servants, members of the patronage service (judicial support staff, including judicial assistants), and other employees of the Supreme Court Staff who use, implement, administer, support or evaluate artificial intelligence systems.

1.3. This Regulation applies to publicly available, enterprise, local, cloud-based and embedded artificial intelligence systems, as well as to systems made available to the Supreme Court within the framework of international technical assistance, research projects or other forms of cooperation.

1.4. This Regulation does not govern the substance of judges' procedural activity in the administration of justice and may not be interpreted as authorising the substitution, restriction or automated formation of judicial discretion.

1.5. Insofar as artificial intelligence systems are used by patronage service staff in preparing cases for consideration, this Regulation shall apply with due regard to the fact that, in such matters, those staff members are accountable to the relevant judge.

2. Legal and Regulatory Framework

2.1. This Regulation shall be applied in accordance with the Constitution of Ukraine; the Laws of Ukraine "On the Judiciary and the Status of Judges", "On Civil Service", "On Information", "On Access to Public Information", "On Access to Court Decisions", "On Personal Data Protection", "On Information Protection in Information and Communication Systems", "On the Basic Principles of Cybersecurity in Ukraine", "On Copyright and Related Rights", and "On Sanctions"; the procedural legislation of Ukraine; international treaties of Ukraine; Article 16 of the Code of Judicial Ethics approved by the decision of the XX Congress of Judges of Ukraine of 18 September 2024; the Regulation on the Supreme Court Staff approved by Resolution No. 6 of the Plenum of the Supreme Court of 30 November 2017; and other acts of the Supreme Court.

2.2. In applying this Regulation, the following may be taken into account as interpretative and practical guidance, insofar as they do not conflict with the legislation of Ukraine:

2.2.1. the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, adopted by the European Commission for the Efficiency of Justice (CEPEJ) in December 2018;

2.2.2. Opinion No. 26 (2023) of the Consultative Council of European Judges, "Moving forward: the use of assistive technology in the judiciary";

2.2.3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence;

2.2.4. the Council of Europe methodology for the risk and impact assessment of artificial intelligence systems from the perspective of human rights, democracy and the rule of law (HUDERIA);

2.2.5. the Guidance on the Responsible Use of Artificial Intelligence by Public Servants, developed by the Ministry of Digital Transformation of Ukraine together with partners in 2025;

2.2.6. the Recommendations for Legal Professionals on the Responsible Use of Artificial Intelligence, prepared by the Ministry of Justice of Ukraine together with national and international partners in 2025;

2.2.7. the Glossary of Terms in the Field of Artificial Intelligence, developed by the Ministry of Digital Transformation of Ukraine together with the Expert Advisory Committee on the Development of Artificial Intelligence in Ukraine, 2024;

2.2.8. the Commentary on the Code of Judicial Ethics, approved by Decision No. 14 of the Council of Judges of Ukraine of 2 March 2026, insofar as it concerns Article 16 of the Code of Judicial Ethics.

3. Key Terms

3.1. For the purposes of this Regulation, the following terms shall have the meanings set out below:

3.1.1. artificial intelligence system (AI system) means a machine-based system that, with a certain degree of autonomy and for explicit or implicit objectives, infers from the input it receives how to generate outputs, including predictions, recommendations, text, images or classifications, that may influence physical or digital environments;

3.1.2. publicly available AI system means a system available to an indefinite range of users in respect of which the Supreme Court has no contract or other legal mechanism governing the processing and protection of official data;

3.1.3. enterprise AI system means a system made available to the Supreme Court on contractual, licensing or other defined legal terms that establish requirements concerning data protection, access and provider responsibility;

3.1.4. local AI system means a system operating within the secure information environment of the Supreme Court without transmitting data to an external provider;

3.1.5. approved use means a defined combination of an AI system, official purpose, categories of data, group of users, technical environment and established restrictions that has been authorised for use by the Supreme Court Staff;

3.1.6. protected data means restricted-access information, as well as other information the use of which is subject to special restrictions under the law or this Regulation, including non-public case materials, internal draft documents, official correspondence, records of official meetings and personal data that have not been lawfully made public;

3.1.7. profiling means automated processing of data concerning a person for the purpose of evaluating or predicting that person's personal, professional, behavioural or other characteristics;

3.1.8. substantial use of an AI system means use that has influenced substantive conclusions, reasoning, selection of sources, assessment of information or another substantive element of an official document or analytical material;

3.1.9. incident means an event related to the use of an AI system that has resulted or could result in the disclosure of protected data, unlawful processing of personal data, use of unreliable output, unauthorised access, a breach of this Regulation or other material harm;

3.1.10. designated organisational unit means one or more organisational units of the Supreme Court Staff designated by the Chief of the Supreme Court Staff to maintain the Register, provide methodological support, conduct risk assessments and monitoring, organise training and respond to incidents;

3.1.11. external AI system means an AI system that uses the technical infrastructure, software environment or services of an external provider to process prompts, data or outputs;

3.1.12. embedded office AI feature means an AI feature integrated into software used by the Supreme Court for drafting, editing, searching, translation, speech-to-text conversion or other technical processing of documents.

3.2. Spell-checking, formatting, technical structuring, automated speech-to-text conversion and preliminary translation without alteration of content do not, in themselves, constitute substantial use of an AI system.

4. Core Principles

4.1. The use of AI systems shall be based on the following principles:

4.1.1. the rule of law, legality and respect for human rights;

4.1.2. judicial independence and non-interference in the administration of justice;

4.1.3. the auxiliary nature of AI systems and mandatory human oversight;

4.1.4. personal responsibility of the employee for the result of his or her work;

4.1.5. accuracy, verifiability and reliance on primary sources;

4.1.6. information protection, cybersecurity and data minimisation;

4.1.7. non-discrimination and prevention of unjustified profiling;

4.1.8. controls proportionate to the level of risk associated with the relevant use;

4.1.9. transparency and the possibility of internal verification of substantial use of AI systems.

Section II. Permitted Use and Prohibitions

5. General Conditions for Permitted Use

5.1. An employee may use an AI system only for an official task falling within that employee's remit, subject to compliance with this Regulation and the restrictions established for the relevant use.

5.2. An AI system shall be used as an auxiliary tool. The employee shall independently determine the content of any document, conclusion or recommendation prepared by that employee. A managerial decision shall be taken by the authorised official, who may not rely exclusively on the output of an AI system.

5.3. Where there is doubt as to whether a system, category of data or use is permissible, the employee shall refrain from such use until clarification is obtained from the designated organisational unit or a decision is taken approving the relevant use.

5.4. Doubts as to whether use of an AI system is permissible shall be resolved in favour of protecting judicial independence, human rights, information security and confidentiality.

5.5. An employee's good-faith refusal to use an AI system because of substantiated concerns regarding safety, legality or the reliability of its output may not, in itself, constitute grounds for a negative assessment of that employee's work, provided that such concerns have been promptly reported to the employee's immediate supervisor or the designated organisational unit.

6. Judicial Independence and Limits on Use in Judicial Activity

6.1. AI systems may not be used to supplant or dictate judicial discretion or a judge's inner conviction, or to automate the assessment of evidence, findings of fact, legal characterisation, formulation of a legal position or determination of the outcome of a specific case.

6.2. It is prohibited to use AI systems for:

6.2.1. automated prediction of the decision of a judge or judicial panel, or of the outcome of a specific case;

6.2.2. modelling the position of a particular judge or judicial panel in a specific case;

6.2.3. automated individual rating, behavioural or predictive assessment of a judge based on the content of judgments, writing style, categories of cases, composition of judicial panels or other parameters;

6.2.4. covert monitoring, emotion recognition, biometric categorisation, or psychological or behavioural profiling of judges;

6.2.5. obtaining, using or disclosing information that, under procedural law, is protected by the confidentiality of judicial decision-making;

6.2.6. creating means of influence, pressure or manipulation directed at judges;

6.2.7. interfering with the automated allocation of court cases or the operation of the court's automated document management system;

6.2.8. automatically generating draft judgments, rulings, separate opinions of judges or other procedural acts;

6.2.9. circumventing established rules on document management, cybersecurity, access control, document approval or other mandatory internal procedures.

6.3. Analytical processing of publicly available case law is permitted for the purposes of summarising case law, identifying systemic legal issues, and preparing statistical, academic and analytical materials, provided that it is not used for individual assessment or prediction of judges' behaviour.

6.4. An AI system may not be used in a manner that covertly omits, selectively presents, ranks or distorts arguments, evidence or legal positions that may be relevant to adversarial proceedings, equality of the parties and the right to a fair trial.

7. Use of AI Systems by Patronage Service Staff

7.1. A member of the patronage service staff may use an AI system in preparing cases for consideration only on the instructions of the relevant judge and within the scope of those instructions. The instructions may relate to a specific case or to defined types of auxiliary tasks in cases of a particular category; they may not expand the uses of AI systems permitted under this Regulation.

7.2. For searching, selecting, summarising and organising publicly available sources, patronage service staff may use AI systems under the same conditions as other employees of the Supreme Court Staff.

7.3. Processing of non-public case materials is permitted only in an approved system within a secure environment and solely for a use entered in the Register.

7.4. Within the scope of paragraph 7.3, the following are permitted:

7.4.1. structuring case materials;

7.4.2. preparing a concise summary of the parties' arguments and objections without evaluating them;

7.4.3. preparing tables, lists and other auxiliary materials;

7.4.4. verifying particulars, references and quotations against official or other reliable primary sources;

7.4.5. technical preparation of descriptive or reference sections of analytical memoranda, reviews, tables and other auxiliary materials without formulating a legal conclusion on behalf of the judge.

7.5. Any concise summary of arguments and objections shall be checked against the original case materials for accuracy and completeness. A material argument or objection may not be omitted solely as a result of automated selection or summarisation.

7.6. An AI system may not independently determine which facts are to be regarded as established, assess evidence, determine its admissibility or sufficiency, formulate a legal conclusion in a specific case, or generate the reasoning or operative part of a judicial decision.

7.7. A draft judicial decision that has not been made public shall, for the purposes of this Regulation, be treated as protected data. Its processing in a publicly available AI system is prohibited. Processing in an enterprise, cloud-based or other external system is permitted only after approval of the relevant use and environment for that category of data. Processing of such a draft in an enterprise, cloud-based or other external system may be approved only subject to compliance with paragraph 15.4 of this Regulation. Embedded office features that meet the requirements of paragraph 10.2 of this Regulation may be applied to a draft judicial decision without separate approval solely for technical spell-checking, formatting and correction of typographical errors, without altering its content. Where the draft or related materials contain information that, under procedural law, is protected by the confidentiality of judicial decision-making, such information may not be processed by an AI system.

7.8. Substantial use of an AI system in preparing for a judge an analytical memorandum, case-law review, selection of sources or other material shall be recorded, and the judge shall be informed of such use in accordance with a procedure approved by the Chief of the Supreme Court Staff. Such notification does not transfer to the judge the employee's responsibility for the accuracy and completeness of the material prepared.

7.9. Information from a closed court hearing may be processed using an AI system only in a local AI system, for a use separately approved for that category of data in accordance with paragraph 20.3 of this Regulation, and on the instructions of the judge before whom the case is pending. Processing such information in an enterprise, cloud-based or other external AI system is prohibited.

8. Permitted Areas of Use

8.1. Subject to compliance with this Regulation, AI systems may be used for:

8.1.1. searching, summarising, classifying and thematically organising publicly available case law, legislation, international instruments, academic materials and other publicly available sources;

- 8.1.2. preparing preliminary analytical, informational, training and reporting materials;
 - 8.1.3. populating and technically organising the Supreme Court Legal Positions Database, provided that each substantive element is verified by an employee before being entered;
 - 8.1.4. technical editing, shortening, structuring and harmonisation of terminology without changing the legal substance;
 - 8.1.5. preliminary translation subject to mandatory professional review;
 - 8.1.6. sorting open data and preparing tables, graphs, charts, templates and other technical materials;
 - 8.1.7. preparing draft information and communication materials that do not contain protected data and do not reflect the Supreme Court's position on the merits of a specific case;
 - 8.1.8. preparing draft responses to applications and requests: where open information is involved, in systems permitted for the relevant level of risk; where protected data are involved, only in an approved secure system;
 - 8.1.9. automated identification of information to be anonymised in the texts of judicial decisions before publication, solely in an approved secure system and subject to mandatory review by an employee;
 - 8.1.10. creating automated information services for matters of a general nature;
 - 8.1.11. other auxiliary tasks, provided that they are not prohibited by this Regulation and comply with the conditions of an approved use.
- 8.2. A text prepared or edited using an AI system shall comply with the standards of the Ukrainian literary language, official and administrative style, legal accuracy, terminological consistency, clarity and concision, as well as the document-formatting rules established by the Supreme Court.
- 8.3. The use of AI systems must not result in plagiarism, concealed borrowing, infringement of copyright or other intellectual property rights, or unjustified transfer to the system provider of rights in official materials.

9. Managerial Decisions and Protection of Employees

- 9.1. A personnel, disciplinary, financial or other managerial decision affecting a person's rights, obligations or legitimate interests may not be taken solely on the basis of a recommendation, assessment, rating or other output of an AI system.
- 9.2. An employee shall be afforded the possibility of human review of an automated recommendation where such a recommendation is used in preparing a managerial decision concerning that employee.
- 9.3. AI systems may not be used for covert monitoring, emotion recognition, biometric categorisation, psychological or behavioural profiling of employees, or for creating automated employee ratings in the absence of a direct legal basis.

10. Publicly Available and Embedded Systems

- 10.1. Without separate approval, publicly available AI systems may be used for low-risk uses involving open information, as specified in paragraph 1 of Appendix 2 and in Appendix 1. Analytical summarisation of publicly available case law or any other substantial use of a publicly available system requires prior approval of the relevant use and its entry in the Register.
- 10.2. Embedded office AI features may be used without separate approval with internal official documents where all of the following conditions are met:

- 10.2.1. the feature does not generate independent legally significant content;
 - 10.2.2. data are not transmitted outside the secure information environment of the Supreme Court or another environment separately authorised for such data;
 - 10.2.3. the feature is not used to analyse the behaviour, productivity or professional qualities of employees or judges;
 - 10.2.4. its use does not affect the rights, obligations or legal position of any person.
- 10.3. Features referred to in paragraph 10.2 may include spell-checking, autocompletion of individual words, technical formatting, detection of typographical errors and other purely technical operations that do not alter the content of the document.

11. Personal Accounts, Automated Speech-to-Text Conversion and Autonomous Tools

- 11.1. For official tasks, personal accounts in AI systems may not be used where protected data or official materials are transmitted to the system. Nor may unapproved software extensions or tools be installed where they have access to official email, documents, calendars or information systems of the Supreme Court.
- 11.2. Automated speech-to-text conversion during official meetings, consultations, videoconferences or other internal discussions is permitted only in an approved system, where there is an official need and subject to compliance with the rules governing access to and retention of the relevant recording.
- 11.3. AI systems capable of independently performing actions on behalf of a user, including sending messages, modifying files, searching internal repositories or interacting with other information systems, may be used only after separate approval and determination of the limits of their authority, access controls and means of terminating their actions.

12. External Communications and AI-Generated Materials

- 12.1. Any material prepared using an AI system for external publication shall undergo substantive, legal and linguistic review by the responsible employee and must not be misleading as to authorship, source, circumstances or the official position of the Supreme Court.
- 12.2. Audio, video or photographic materials generated using AI systems that imitate a specific judge or employee of the Supreme Court and may be perceived as authentic may be created or disseminated only with that person's prior consent and subject to appropriate labelling.
- 12.3. It is prohibited to create materials that imitate an official communication or position of the Supreme Court and may be perceived as authentic.

13. Automated Information Services

- 13.1. Automated information services may provide general information about the activities of the Supreme Court, procedures for contacting the Court, guidance on navigating its official electronic resources, and other information of a general nature.
- 13.2. Such services may not provide legal advice concerning a specific case, predict the outcome of a case, create the impression that the user is communicating with a judge or an authorised employee, or present their output as the official position of the Court.
- 13.3. Before interaction begins, the user shall be clearly informed that the user is interacting with an automated service and that its responses are for informational purposes only.

13.4. The user shall be provided with a clear means of contacting an authorised employee of the Supreme Court in relation to a matter that falls outside the scope of the service's information function.

14. Verification of Outputs and Recording of Substantial Use

14.1. The output of an AI system has no independent evidentiary, normative or official force and does not constitute a primary source.

14.2. Before using AI-generated output in official work, an employee shall verify factual data, sources, quotations, particulars, dates, translations and legal conclusions against official or other reliable primary sources. In the case of a normative legal act, the employee shall verify its validity and the version applicable to the matter; in the case of a judicial decision, the employee shall verify its current status and, where necessary, whether the relevant legal position has been departed from or modified.

14.3. Where an output contains a concise summary of a document, arguments or a substantial body of information, the employee shall verify not only the accuracy but also the completeness with which material points are reflected.

14.4. Unverified information may not be presented as reliable. Where a source or statement cannot be verified, it shall not be used as confirmed information.

14.5. Substantial use of an AI system in material transmitted to a judge or in a document intended for an external recipient shall be recorded in accordance with a procedure approved by the Chief of the Supreme Court Staff.

14.6. Substantial use of an AI system in a document sent to an external recipient or made public shall be disclosed in the document itself or in accompanying information, unless otherwise provided by law. Such disclosure is not required where the AI system was used solely for operations specified in paragraph 3.2 of this Regulation.

14.7. Recording and notifying the recipient do not relieve the employee of the duty to verify the material and do not transfer responsibility for the content of the material prepared to the recipient.

14.8. A preliminary translation produced by an AI system shall be subject to professional review. It does not replace a professional translation where such translation is required by law or by the nature of the document and may not be presented as a final official text without review by an authorised person.

14.9. Where, in the course of permitted processing of case materials, an employee identifies in a document submitted by a party a reference to a non-existent judicial decision, normative legal act or other source, or a materially distorted quotation, the employee shall verify the relevant information, record the discrepancy identified and inform the judge, without making assumptions as to the reasons for its occurrence.

Section III. Data, External Systems and Cybersecurity

15. Data Processing and Conditions for the Use of External Systems

15.1. Processing of protected data using an AI system is permitted only where there is a legal basis, an official need and an approved use in a secure environment, except in cases expressly provided for in paragraphs 7.7 and 10.2 of this Regulation.

15.2. Non-public case materials, internal draft documents, official correspondence, records of internal meetings, information from closed court hearings, restricted-access information and other protected data may not be entered into publicly available AI systems.

15.3. Publicly available personal data or case numbers that have already been made public may be used only where there is an official purpose and only to the extent necessary for the relevant task. Data which, when combined, disclose non-public context concerning a specific case or person may not be entered into publicly available systems.

15.4. Where protected data are processed in an external AI system, the conditions governing its use must exclude the use of input data, prompts and outputs for the training or improvement of models by the provider or third parties. Retention periods for such data shall be minimised; provider and third-party access shall be restricted by technical and organisational measures; and the procedures governing access, logging and deletion of the data shall be determined before the system is used. When working with open information, settings that prevent the use of input data, prompts and outputs for model training or improvement shall be applied where technically available.

15.5. An external system may not be used where its terms provide for unjustified assignment of proprietary rights in official materials, use of official materials to train commercial models without the authorisation of the Supreme Court, uncontrolled transfer of data to third parties, or an undefined data-retention and deletion regime. Protected data may under no circumstances be used to train or improve models.

15.6. Prompts, outputs and event logs shall be retained no longer than necessary for the specified official, security or control purpose, unless a different retention period is prescribed by law. For each approved use, retention periods, deletion procedures, persons entitled to access and, where necessary, backup arrangements shall be defined.

16. Cybersecurity Requirements

16.1. The following threats, among others, shall be taken into account when AI systems are implemented and used:

16.1.1. unauthorised access and data leakage;

16.1.2. hidden or malicious instructions in documents, webpages or other input data intended to alter system behaviour or circumvent established restrictions;

16.1.3. deliberate distortion, substitution or contamination of data and sources used by the system;

16.1.4. substitution or unauthorised alteration of system outputs;

16.1.5. disclosure of official information through event logs, system messages, feedback channels or external system components;

16.1.6. risks associated with updates, connections to external services and autonomous performance of actions.

16.2. For medium- and high-risk uses, at least the following shall be established:

16.2.1. procedures for user authentication and access control;

16.2.2. rules governing the entry, uploading and transmission of data;

16.2.3. maintenance of event logs to the extent necessary and proportionate;

16.2.4. procedures for reviewing updates, external components and connections to other information systems;

16.2.5. procedures for data retention, deletion, backup and recovery;

16.2.6. procedures for responding to failures, suspicious outputs and incidents;

16.2.7. the ability to immediately restrict access to or terminate operation of the system.

17. Providers, Sanctions and Jurisdictional Risks

17.1. A system may not be used where it is impossible to establish its provider, the principal conditions governing data processing, the procedure for third-party access or the legal regime applicable to data retention to the extent necessary for a security assessment.

17.2. Use of an AI system is prohibited where its provider, owner or any person exercising decisive influence over such provider or owner is an aggressor state or occupying state, a state authority thereof, a legal person established under the law of such a state or registered in its territory, a natural person who is a citizen or resident of such a state, or another person in respect of whom the law of Ukraine prohibits the relevant use. The prohibition shall also apply where key infrastructure of the system is located in the territory of an aggressor state or occupying state.

17.3. Where sanctions have been imposed on the provider, owner, controller, beneficial owner of the system or persons associated with it, the permissibility of using the system shall be determined in accordance with the content and scope of the relevant sanctions and the requirements of Ukrainian law.

17.4. In other cases, the risk of access by a foreign state to official information shall be assessed having regard to the provider's jurisdiction and the place of data processing, applicable law, contractual and technical safeguards, categories of data, and recommendations of the State Service of Special Communications and Information Protection of Ukraine and other competent cybersecurity authorities. The mere use of foreign cloud infrastructure shall not, in itself, constitute sufficient grounds for prohibition.

Section IV. Risk Assessment, Approval and the Register

18. Risk Levels for Uses of AI Systems

18.1. Risk shall be assessed in relation to a specific use of an AI system, taking into account the official purpose, categories of data, level of autonomy, technical environment, potential impact on individual rights, the interests of justice, judicial independence and information security.

18.2. Low-risk use includes technical, linguistic, reference or training tasks that do not generate legally significant content and do not affect the rights or obligations of persons.

18.3. Medium-risk use includes, in particular, the preparation of preliminary analytical materials, summarisation of publicly available case law, processing of large volumes of open information, preparation of external information materials and other tasks in which the output of an AI system may materially influence the content of an official material.

18.4. High-risk use includes uses involving substantive processing of protected data, other than purely technical operations permitted under paragraph 10.2 of this Regulation; work in critical or important information systems; autonomous performance of actions; material influence on managerial processes; or a potential impact on the rights, interests or legal position of persons.

18.5. A use prohibited by this Regulation may not be approved irrespective of the assessed level of risk.

19. Register of Approved Uses of AI Systems

19.1. The Supreme Court Staff shall maintain a Register of Approved Uses of AI Systems.

19.2. The Register shall contain at least the information specified in Appendix 3.

19.3. The Register shall be maintained by the designated organisational unit. The procedure for maintaining the Register and the levels of access to it shall be approved by the Chief of the Supreme Court Staff.

20. Approval and Reassessment

20.1. Only uses expressly identified in this Regulation and Appendix 1 as not requiring approval may be carried out without separate approval.

20.2. Other uses shall be permitted only after approval by the Chief of the Supreme Court Staff on the submission of the designated organisational unit and after entry in the Register.

20.3. Where a use concerns the preparation of cases for consideration by patronage service staff, the general conditions for such use shall be approved following agreement with the President of the Supreme Court, and use in a specific case shall be permitted only on the instructions of the relevant judge.

20.4. Following the assessment, a decision may be taken to:

20.4.1. permit use within defined limits;

20.4.2. permit use subject to additional restrictions or safeguards;

20.4.3. permit pilot use for a specified period and for a specified group of users;

20.4.4. refuse approval;

20.4.5. suspend or terminate a previously approved use.

20.5. Before approval, the following shall be assessed: the purpose and functions of the system; categories of data; conditions of storage and transmission; third-party access; the possibility of using data to train the model; contractual terms or terms of use; cybersecurity measures; risks of errors and bias; the ability to terminate use; and, for high-risk uses, the impact on human rights.

20.6. For high-risk uses, before approval the system's resilience to erroneous, manipulative and malicious inputs, attempts to circumvent established restrictions and unauthorised access shall be assessed, including by reference to the results of testing conducted by the provider, an independent organisation or the designated organisational unit.

20.7. A material change in the model, functions, data-processing conditions, technical environment, categories of users or risk level shall trigger reassessment. Pending completion of the reassessment, use may be restricted or suspended.

Section V. Monitoring, Audit and Incidents

21. Monitoring and Audit

21.1. Monitoring of the use of approved AI systems shall be conducted solely for the purposes of ensuring security, verifying compliance with this Regulation, evaluating system performance and responding to incidents.

21.2. Monitoring may not be used as a covert means of assessing the productivity, behaviour or professional qualities of employees or judges.

21.3. Employees shall be informed of the purpose of event logging, the categories of data recorded, retention periods, persons with access and the manner in which the relevant information is used.

21.4. Use of AI systems may be subject to internal audit. On the basis of the audit findings, the conditions of approval may be amended, use of a system may be suspended or terminated, and additional safeguards or training measures may be prescribed.

22. Incidents

22.1. An employee shall immediately report an incident or a substantiated suspicion of an incident to the employee's immediate supervisor and the designated organisational unit.

22.2. Initial response measures may include terminating or suspending use of the system, restricting access, recording the circumstances, assessing a possible data leak or unlawful processing, correcting unreliable information and notifying the responsible units.

22.3. The procedure for responding to incidents, reporting deadlines, responsible persons and documentation requirements shall be approved by the Chief of the Supreme Court Staff. The employee's initial actions are set out in Appendix 4.

Section VI. Training, Transparency, Responsibility, Review and Entry into Force

23. Employee Training

23.1. Employees who use or may use AI systems in the course of their official duties shall undergo periodic training or instruction organised by the Supreme Court, including in cooperation with the National School of Judges of Ukraine.

23.2. Training shall cover the rules set out in this Regulation; the principal capabilities and limitations of AI systems; data protection; verification of outputs against primary sources; safe formulation of prompts; indicators of unreliable outputs; the risks of overreliance on automated outputs and of AI systems tailoring responses to the user's expectations; cybersecurity threats; procedures for recording substantial use; and incident response.

24. Transparency of Information on the Use of AI Systems

24.1. On the basis of monitoring and audit results, the Supreme Court Staff shall, at least once a year, prepare and publish on the official website of the Supreme Court a consolidated report on the use of AI systems containing information on areas of use, approved uses, results of application, effectiveness, identified risks, safeguards implemented, training conducted and aggregated information on incidents.

24.2. The report may not contain restricted-access information, personal data, details of technical vulnerabilities or other information the disclosure of which could pose a threat to the security of the Supreme Court.

24.3. Publication of information on the use of AI systems must not create a misleading impression that AI systems may be used to formulate judicial decisions or replace judicial discretion.

24.4. This Regulation may be the subject of consultation with judges, academics, members of the Bar, specialists in information security, personal data protection and artificial intelligence, and the public.

25. Responsibility

25.1. A breach of this Regulation may be taken into account in determining responsibility only in the cases and in accordance with the procedures prescribed by law, having regard to the legal status of the employee concerned.

25.2. In assessing an employee's conduct, regard shall be had to the nature and consequences of the breach, the form of fault, official duties, whether the incident was reported promptly, and the measures taken to prevent or remedy harm.

26. Review, Appendices and Entry into Force

26.1. This Regulation shall be reviewed periodically, taking into account changes in legislation, technological developments, international standards, the practice of the Supreme Court, monitoring results and incidents.

26.2. When this Regulation is reviewed, account shall be taken of the documents referred to in paragraph 2.2, as well as new documents of the Council of Europe, the European Commission for the Efficiency of Justice, the European Union, UNESCO and competent Ukrainian authorities in the field of artificial intelligence and justice.

26.3. Appendices 1 to 4 form an integral part of this Regulation. In the event of any inconsistency between the text of this Regulation and an Appendix, the text of this Regulation shall prevail.

26.4. This Regulation shall be approved by an order of the Chief of the Supreme Court Staff following agreement with the President of the Supreme Court and shall enter into force on the date specified in that order.

26.5. Within the period specified in the order approving this Regulation, the designated organisational unit shall conduct an inventory of AI systems actually used by the Supreme Court Staff and shall arrange for the assessment of the relevant uses, their entry in the Register or the preparation of proposals to discontinue their use. AI technologies approved by the Chief of the Supreme Court Staff pursuant to subparagraph 3 of paragraph 2 of Section IV of the Regulation approved by Order No. 117 of the Chief of the Supreme Court Staff dated 8 December 2025 shall, during the inventory, be assessed as a matter of priority in accordance with this Regulation.

26.6. Pending completion of the inventory:

26.6.1. publicly available systems may be used only for low-risk uses involving open information;

26.6.2. AI technologies approved pursuant to subparagraph 3 of paragraph 2 of Section IV of the Regulation approved by Order No. 117 of the Chief of the Supreme Court Staff dated 8 December 2025 may continue to be used within the scope and under the conditions specified in the relevant approval decision until their assessment is completed, but no longer than the inventory period;

26.6.3. other existing enterprise systems may temporarily be used within the scope of existing contracts and settings only for low-risk uses and without processing protected data;

26.6.4. embedded office features may be used in accordance with paragraph 10.2 of this Regulation;

26.6.5. other medium- and high-risk uses shall be permitted only after approval in accordance with this Regulation.

Appendix 1. Matrix of Permitted Uses of AI Systems

The Matrix shall be applied together with the text of this Regulation. The designation "subject to approval" means approval of the specific use and its entry in the Register.

Type of data or task	Publicly available system	Enterprise / cloud-based system	Local secure system	Embedded office feature
Spell-checking and formatting of open text	permitted	permitted	permitted	permitted
Other low-risk uses involving open information (Appendix 2, paragraph 1)	permitted	permitted	permitted	permitted
Analytical summarisation of publicly available case law	subject to approval	subject to approval	subject to approval	subject to approval where the feature materially affects content
Publicly available personal data and case numbers of published cases	only where officially necessary and to the minimum extent required	in accordance with the approved use	in accordance with the approved use	only where data are not transmitted outside the authorised environment
Internal official document containing no restricted-access information	prohibited	subject to approval	subject to approval	permitted only subject to paragraph 10.2
Personal data that have not been lawfully made public	prohibited	subject to approval where there is a legal basis	subject to approval where there is a legal basis	only subject to paragraph 10.2 and appropriate protection
Non-public case materials	prohibited	subject to approval in a secure environment	subject to approval	subject to approval where the feature processes the content of case materials
Information from a closed court hearing	prohibited	prohibited	only subject to paragraph 7.9	only where the feature operates in a local environment and the requirements of paragraphs 7.9 and 10.2 are met
Unpublished draft judicial decision	prohibited	subject to approval under paragraph 7.7	subject to approval; technical features under paragraph 10.2	permitted for purely technical operations under paragraphs 7.7 and 10.2

Type of data or task	Publicly available system	Enterprise / cloud-based system	Local secure system	Embedded office feature
Information protected by the confidentiality of judicial decision-making	prohibited	prohibited	prohibited	prohibited
Automated speech-to-text conversion of an official meeting	prohibited	subject approval to	subject approval to	subject approval to
Automated anonymisation of a judicial decision before publication	prohibited	subject approval to	subject approval to	subject approval to

Appendix 2. Typical Uses by Risk Level

1. Low risk: spell-checking, formatting, preliminary translation of open text, technical structuring, creation of tables from open data, and reference searches in open sources.
2. Medium risk: summarisation of publicly available case law, preparation of preliminary analytical material, thematic grouping of large bodies of open-source material, and preparation of external information material involving substantial use of an AI system.
3. High risk: processing of non-public case materials, automated anonymisation of judicial decisions before publication, connection to internal information systems, autonomous performance of actions, or substantive processing of other protected data, except for purely technical operations permitted under paragraph 10.2 of this Regulation.
4. Prohibited use means any use of AI systems prohibited by this Regulation, including the uses specified in paragraphs 6, 9 and 12. Such uses include, in particular, predicting the outcome of a specific case, formulating a legal position in place of a judge, automatically generating procedural acts, profiling judges, covertly or selectively filtering out material arguments, processing information protected by the confidentiality of judicial decision-making, interfering with the automated allocation of cases, covert monitoring, emotion recognition, biometric categorisation, and creating misleading synthetic content.

Appendix 3. Minimum Information to Be Included in the Register

1. name of the system and provider;
2. description of the approved use;
3. official purpose;
4. categories of users;
5. categories of data that may and may not be processed;
6. technical environment;
7. risk level and the results of assessments and tests carried out in accordance with paragraphs 17, 18, 20.5 and 20.6 of this Regulation;
8. type of decision taken in accordance with paragraph 20.4 of this Regulation;

9. in the case of pilot use, the duration of such use and the group of users;
10. in the cases provided for in paragraph 20.3 of this Regulation, information on agreement with the President of the Supreme Court;
11. restrictions and mandatory safeguards;
12. retention periods for prompts, outputs and event logs;
13. designated organisational unit;
14. date of approval and date of the next review;
15. information on suspension, termination or reassessment.

Appendix 4. Initial Actions in the Event of an Incident

1. stop any action that may aggravate the consequences of the incident;
2. immediately notify the immediate supervisor and the designated organisational unit;
3. where the incident concerns the materials of a specific court case, immediately notify the judge before whom the case is pending or another judge of the relevant judicial panel as determined by the internal procedure;
4. record the time, system, nature of the data and the known circumstances of the event;
5. do not delete event logs or other information necessary for review, unless retaining them would increase the risk;
6. follow any further instructions of the designated organisational unit concerning access restrictions, remediation, notification of other persons or termination of use of the system.