

Draft Regulation on Responsible AI Use by Supreme Court Staff

Author: Bernaziuk Ian

Affiliation: Supreme Court

Publication: Конституціоналіст · 2026

Publication date: 2026-06-19

Permanent URL: <https://constitutionalist.com.ua/draft-regulation-on-responsible-ai-use-by-supreme-court-staff/>

Author information

Bernaziuk Ian

Supreme Court

Document text

Draft for Professional and Public Discussion

REGULATION

on the Use of Artificial Intelligence Technologies by Employees of the Supreme Court Staff

Section I. General Provisions

Article 1. Subject Matter

1.1. This Regulation defines the legal, organisational, ethical and security principles governing the use of artificial intelligence technologies by employees of the Supreme Court Staff in the performance of their official duties.

1.2. This Regulation establishes:

1.2.1. the fundamental principles of responsible use of artificial intelligence technologies;

1.2.2. the permitted areas and limits of use of artificial intelligence technologies;

1.2.3. prohibitions and restrictions aimed at protecting judicial independence, the confidentiality of judicial deliberations, restricted-access information, personal data, human rights and freedoms, and trust in the Supreme Court;

1.2.4. requirements for the approval, recording, use, monitoring and audit of artificial intelligence systems;

1.2.5. the procedure for verifying results obtained through the use of artificial intelligence technologies;

1.2.6. rules for responding to incidents related to the use of artificial intelligence technologies;

1.2.7. the general principles of liability of employees for violations of this Regulation.

1.3. This Regulation is an internal organisational act of the Supreme Court and 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 Personal Data Protection”, “On Protection of Information in Information and Communication Systems”, “On the Basic Principles of Ensuring Cybersecurity of Ukraine”, procedural legislation of Ukraine, international treaties to which the Verkhovna Rada of Ukraine has given consent to be bound, acts of the Supreme Court, and taking into account relevant international standards for the responsible use of artificial intelligence technologies in the field of justice.

Article 2. Purpose of the Regulation

2.1. The purpose of this Regulation is to create proper, safe, transparent and responsible conditions for the use of artificial intelligence technologies in the activities of the Supreme Court Staff in order to improve the quality, timeliness and efficiency of specific work processes without prejudice to judicial independence, human rights, information security and public trust in the Supreme Court.

2.2. This Regulation is aimed at ensuring an approach to the use of artificial intelligence technologies under which the Supreme Court:

2.2.1. recognises the potential of artificial intelligence technologies to improve the analytical, informational, organisational, communication, translation, training and technical activities of the Staff;

2.2.2. uses artificial intelligence technologies only as an auxiliary tool that does not replace human critical thinking, professional judgement, legal characterisation, professional experience or the employee's personal responsibility;

2.2.3. does not allow the use of artificial intelligence technologies in a manner that may directly or indirectly affect the administration of justice, the judge's inner conviction, the confidentiality of judicial deliberations or the content of a judicial decision;

2.2.4. ensures the protection of restricted-access information, personal data, official information, case-file materials and internal documents of the Supreme Court;

2.2.5. develops a modern, responsible model for the use of artificial intelligence technologies in judicial administration that is oriented towards maintaining public trust.

Article 3. Scope of the Regulation

3.1. This Regulation applies to all civil servants and employees of the Supreme Court Staff who use, intend to use, initiate the implementation of, administer, support or assess artificial intelligence systems within the scope of their official activities.

3.2. This Regulation applies to the use of:

3.2.1. publicly available artificial intelligence systems;

3.2.2. corporate, licensed or cloud-based artificial intelligence systems to which the Supreme Court has been granted access;

3.2.3. local artificial intelligence systems deployed within the protected information environment of the Supreme Court;

3.2.4. artificial intelligence systems provided to the Supreme Court within the framework of international technical assistance, grant programmes, pilot projects, memoranda or other forms of cooperation with third parties;

3.2.5. artificial intelligence functions embedded in software, including intelligent search, autocomplete, automatic text correction, transcription, translation, summarisation, classification and generation of text, images, audio, video or program code.

3.3. This Regulation does not govern the substance of the procedural activities of judges of the Supreme Court in the administration of justice.

3.4. No provision of this document may be interpreted as authorising the use of artificial intelligence technologies to replace judicial discretion, the assessment of evidence, the establishment of factual circumstances of a case, the formation of a judge's legal position, the rendering of a judicial decision or the determination of the outcome of a particular case.

3.5. The use of artificial intelligence technologies by employees of the Supreme Court Staff shall not directly or indirectly affect:

3.5.1. the independence, impartiality and absence of bias of judges of the Supreme Court;

3.5.2. the procedure for determining the composition of a court;

3.5.3. the automated allocation of court cases;

3.5.4. the confidentiality of judicial deliberations;

3.5.5. the internal process by which a judge forms his or her conviction;

3.5.6. the content of judicial decisions or the final legal positions of the court.

3.6. In the event of doubt as to the permissibility of using a particular artificial intelligence system, type of data, method of data processing or nature of an official task, an employee shall refrain from such use until clarification or permission is obtained from the immediate supervisor or the authorised structural unit.

3.7. All doubts concerning the permissibility of using artificial intelligence technologies shall be interpreted in favour of protecting judicial independence, human rights and freedoms, information security, personal data, confidentiality and public trust in the Supreme Court.

Section II. Definitions of Key Terms

Article 4. Terms Used in this Regulation

4.1. For the purposes of this Regulation, the terms below shall have the following meanings:

4.1.1. artificial intelligence technologies means software systems, models, tools or digital services which, on the basis of input data, instructions, prompts, documents or other materials, are capable of generating, classifying, predicting, summarising, translating, analysing, structuring or otherwise processing information using algorithmic methods, machine learning, large language models or other related technologies;

4.1.2. artificial intelligence system or AI system means a separate software product, service, model, function, platform or tool that implements artificial intelligence technologies;

4.1.3. generative artificial intelligence system means an artificial intelligence system capable of creating new text, images, audio, video, program code, a document structure, analytical summary or other content on the basis of a user prompt;

4.1.4. publicly available artificial intelligence system means an artificial intelligence system to which access is provided publicly, without a contract or other legal instrument concluded by the Supreme Court that defines the regime for processing input data, guarantees for its protection, storage conditions and restrictions on third-party access;

4.1.5. corporate artificial intelligence system means an artificial intelligence system to which the Supreme Court has been granted access on contractual, licensing or other defined legal grounds, with established conditions for security, data processing, provider liability and access control;

4.1.6. local artificial intelligence system means an artificial intelligence system operating within the protected information environment of the Supreme Court without transferring data to external providers, unless otherwise expressly permitted by a relevant decision of the Head of the Supreme Court Staff;

4.1.7. protected information environment of the Supreme Court means a set of organisational, technical, software and security measures that ensure controlled access, protection, isolation, recording and secure processing of information in the information systems of the Supreme Court;

4.1.8. approved artificial intelligence system means an artificial intelligence system whose use within defined limits is authorised in the Supreme Court Staff and which has been entered in the Register of Approved Artificial Intelligence Systems;

4.1.9. restricted-access information means confidential, secret and official information within the meaning of Ukrainian legislation, including personal data, banking, advocate-client, medical, notarial, commercial and other legally protected secrets, information from court case files, information from closed court hearings, the confidentiality

of judicial deliberations, internal draft documents, official correspondence, records of official meetings, consultations and internal discussions, where access to such information is restricted by law or by internal acts of the Supreme Court;

4.1.10. prompt to an artificial intelligence system means an instruction, text, document, question, command, data or other input materials entered, uploaded or transmitted by a user to an artificial intelligence system in order to obtain a result;

4.1.11. output of an artificial intelligence system means text, an answer, conclusion, structure, translation, classification, table, chart, image, audio, video, program code or other content created, modified, organised or proposed by an artificial intelligence system;

4.1.12. hallucination of an artificial intelligence system means an unreliable, wholly or partly fabricated, incomplete, distorted or unverifiable output generated by an artificial intelligence system that has external features of reliable information, including non-existent legal acts, fabricated judicial decisions, incorrect particulars, inaccurate or out-of-context quotations, or erroneous legal conclusions;

4.1.13. profiling means any form of automated processing of personal data or other information concerning a person which consists of using such data or information to assess, analyse or predict personal, psychological, behavioural, professional or other characteristics of that person, including his or her decisions, writing style, productivity, inclinations or possible actions;

4.1.14. synthetic content means text, audio, video, photographic or other materials created or materially altered by artificial intelligence tools and capable of imitating real persons, their statements, actions, positions or official communications;

4.1.15. risk level of an artificial intelligence system means the classification of an artificial intelligence system as a low-, medium- or high-risk system depending on the purpose of its use, the type of data, the technical environment, the level of autonomy, the possible impact on the rights of persons, the interests of justice, judicial independence, information security and trust in the Supreme Court;

4.1.16. incident related to the use of artificial intelligence means an event or a set of events that has led or could lead to the disclosure of restricted-access information, unlawful processing of personal data, use of an unreliable output, violation of this Regulation, technical vulnerability, unauthorised access, or the creation of a risk to human rights, judicial independence, the security of the Supreme Court or trust in the judiciary;

4.1.17. substantial use of artificial intelligence technologies means the use of an artificial intelligence system where its output has influenced the content, structure, conclusions, reasoning, selection of sources, summary of information or another substantive element of an official document, analytical material, response, report, presentation or other result of official activity; the use of artificial intelligence technologies exclusively for spell-checking, formatting, technical error detection, improving readability without changing content, or another auxiliary technical action shall not constitute substantial use;

4.1.18. external artificial intelligence system means an artificial intelligence system that is not fully deployed within the protected information environment of the Supreme Court and that involves the processing of prompts, data or outputs through the use of the technical infrastructure, software environment or services of an external provider;

4.1.19. authorised structural unit means a structural unit of the Supreme Court Staff, or several structural units, designated by the Head of the Supreme Court Staff to provide methodological support, maintain the Register, organise monitoring, audit, training, incident response or perform other tasks provided for by this Regulation.

4.2. Terms not defined in this Regulation shall be used in the meanings established by Ukrainian legislation and relevant national and international standards in the field of responsible use of artificial intelligence technologies.

Section III. Fundamental Principles of Responsible Use of Artificial Intelligence Technologies

Article 5. General Principles

5.1. The use of artificial intelligence technologies by employees of the Supreme Court Staff shall be based on the following principles:

- 5.1.1. the rule of law, legality and respect for human rights;
- 5.1.2. judicial independence and non-interference in the administration of justice;
- 5.1.3. the auxiliary nature of artificial intelligence technologies;
- 5.1.4. human oversight and personal responsibility;
- 5.1.5. confidentiality, cybersecurity and protection of restricted-access information;
- 5.1.6. reliability, verifiability and good faith;
- 5.1.7. non-discrimination, fairness and minimisation of algorithmic bias;
- 5.1.8. proportionality, data minimisation and a risk-based approach;
- 5.1.9. transparency at an appropriate level and traceability of use;
- 5.1.10. preservation of the official style, professional language and institutional authenticity of the Supreme Court.

Article 6. Rule of Law, Legality and Respect for Human Rights

6.1. The use of artificial intelligence technologies shall comply with the Constitution of Ukraine, the laws of Ukraine, Ukraine's international obligations, and standards of fair trial, privacy protection, personal data protection, equality, non-discrimination, access to justice and legal certainty.

6.2. Artificial intelligence technologies may not be used in a manner that creates a risk of:

- 6.2.1. undermining human dignity;
- 6.2.2. infringing privacy or unlawfully processing personal data;
- 6.2.3. discrimination or disproportionate impact on particular groups of persons;
- 6.2.4. manipulative influence on a person;
- 6.2.5. covert surveillance or unjustified profiling;
- 6.2.6. restricting access to a court;
- 6.2.7. undermining trust in the Supreme Court or the judiciary.

Article 7. Judicial Independence and Non-Interference in the Administration of Justice

7.1. The use of artificial intelligence technologies in the Supreme Court Staff may not have the purpose or effect of influencing judicial independence, the judge's inner conviction, the assessment of evidence, the legal characterisation of the circumstances of a case, the content of a judicial decision or the outcome of a particular case.

7.2. The use of artificial intelligence systems is prohibited for:

- 7.2.1. predictive analysis of individual judicial activity;
- 7.2.2. psychological, professional, behavioural or statistical profiling of judges of the Supreme Court;

- 7.2.3. automated forecasting of probable outcomes of particular court cases;
- 7.2.4. modelling the position of a judge or a judicial panel in a particular case;
- 7.2.5. evaluating a judge on the basis of the content of his or her judicial decisions, writing style, previous decisions, composition of panels, categories of cases or other parameters;
- 7.2.6. creating tools of direct or indirect influence, pressure or manipulation in relation to judges.
- 7.3. Analytical processing of open judicial practice is permissible only where it is aimed at ensuring the unity of judicial practice, identifying systemic legal problems, preparing summaries, statistical or academic analytical materials, and is not used to forecast or evaluate the individual behaviour of judges.
- 7.4. Artificial intelligence systems used for analytical processing, summarisation or structuring of information may not be applied in a manner that covertly limits, selectively presents, filters, ranks or distorts legal arguments, submissions or positions relevant to ensuring adversarial proceedings, equality of arms, access to justice and the right to a fair trial.

Article 8. Auxiliary Nature of Artificial Intelligence

- 8.1. Artificial intelligence systems may be used only as auxiliary tools to support an employee in performing permitted official tasks.
- 8.2. Artificial intelligence systems may not independently determine the content of an official document, legal position, conclusion, recommendation, response, assessment or managerial decision.
- 8.3. No organisational, administrative, personnel, disciplinary, financial, logistical or other official decision within the Supreme Court Staff may be adopted exclusively on the basis of recommendations, calculations, assessments, ratings, forecasts or analytical conclusions generated by artificial intelligence systems.
- 8.4. Where artificial intelligence systems are used to automate internal administrative processes, preliminarily sort documents, classify requests or allocate technical tasks, the outputs generated by such systems shall be exclusively auxiliary in nature. An employee has the right to apply to his or her immediate supervisor for human review, clarification or correction of the relevant automated recommendation, and the final managerial decision shall be taken by an authorised official.

Article 9. Human Oversight and Personal Responsibility

- 9.1. An employee who uses artificial intelligence technologies shall independently and critically assess the appropriateness of such use, formulate prompts, verify the outputs obtained and be responsible for their accuracy, completeness, legality, ethical propriety and suitability for further use.
- 9.2. The use of artificial intelligence technologies does not release an employee from personal responsibility for the results of his or her work.
- 9.3. Blind or uncritical acceptance of options proposed by an artificial intelligence system concerning legal characterisation, interpretation of legal provisions, assessment of arguments, summarisation of judicial practice, factual conclusions, quotations, particulars or textual wording shall not be permitted.
- 9.4. Mechanical transfer of the output of an artificial intelligence system into an official document without proper professional verification, substantive processing and alignment with the standards of the Supreme Court may, depending on the nature of the violation and its consequences, be regarded as improper performance of official duties.
- 9.5. A good-faith refusal by an employee to use artificial intelligence technologies on the grounds provided for by this Regulation, including justified doubts as to the permissibility of such use, the reliability of the output or the security of data processing, may not in itself serve as a basis for a negative assessment of that employee's work, provided that the employee has timely notified his or her immediate supervisor or the authorised structural unit of such doubts.

Article 10. Confidentiality, Cybersecurity and Information Protection

10.1. When using artificial intelligence technologies, an employee shall ensure non-disclosure of restricted-access information.

10.2. Publicly available artificial intelligence systems shall not be used to process:

10.2.1. court case-file materials;

10.2.2. official documents that are not publicly available;

10.2.3. internal draft documents;

10.2.4. official correspondence;

10.2.5. personal data;

10.2.6. information from closed court hearings;

10.2.7. records of official meetings, consultations or internal discussions;

10.2.8. the confidentiality of judicial deliberations;

10.2.9. banking, advocate-client, medical, commercial or other legally protected secrets;

10.2.10. any other information whose disclosure may harm the rights of persons, the interests of justice, the security of the Supreme Court or trust in the judiciary.

10.3. Prompts to artificial intelligence systems shall be formulated in anonymised, generalised and minimally necessary form.

10.4. It is prohibited to enter into artificial intelligence systems combinations of non-public facts, dates, procedural statuses, positions, amounts, locations, particulars or other information which, taken together, make it possible to identify a specific court case, person, official discussion, internal document or position of the court, even where direct identifiers are not specified.

Article 11. Reliability, Verifiability and Good Faith

11.1. Any information created, modified, summarised or proposed by an artificial intelligence system shall be subject to professional verification by the employee before it is used in official activity.

11.2. Factual data, quotations, references to legal acts, judicial practice, international documents, academic sources, statistical indicators, names, dates, particulars and conclusions obtained with the help of artificial intelligence technologies shall be verified against official or other reliable primary sources.

11.3. The employee shall personally ascertain the existence of the relevant source, the accuracy of the quoted text, the validity of the legal act, the current relevance of the judicial decision, the accuracy of the translation and the absence of distortion of meaning.

11.4. Where the reliability of a source, fact, quotation, particular, legal conclusion or other information proposed by an artificial intelligence system cannot be verified, such information may not be used as confirmed.

11.5. When using approved analytical artificial intelligence systems to summarise large datasets of judicial decisions or other open legal sources, the employee shall conduct a selective verification of the representativeness of the output obtained. Where there are signs of systematic disregard of relevant legal positions, references to invalid or repealed acts, distortion of the content of sources or another material error, the employee shall refrain from using such output as confirmed and shall notify the authorised structural unit.

Article 12. Non-Discrimination, Fairness and Minimisation of Algorithmic Bias

12.1. When selecting, implementing and using artificial intelligence systems, the Supreme Court Staff shall take reasonable measures to identify, minimise and prevent systemic errors, hidden discrimination, disproportionate impact on particular groups of persons or the reproduction of biases.

12.2. The use of artificial intelligence systems shall not be permitted where their application creates a disproportionate risk of discrimination, violation of equality, stigmatisation, unjustified profiling or another unfair impact on a person.

12.3. When approving artificial intelligence systems, consideration shall be given to the availability of information about the purpose of the system, the main limitations of its use, known risks, the procedure for data processing and measures to minimise errors and bias.

Article 13. Proportionality, Data Minimisation and Risk-Based Approach

13.1. For the performance of an official task using artificial intelligence technologies, an employee shall use only those data that are necessary, sufficient and permissible for the relevant purpose.

13.2. The amount of data entered into an artificial intelligence system shall be minimal and shall not exceed the limits necessary to achieve a lawful and officially justified purpose.

13.3. Requirements for security, approval, control, recording, logging, audit and reporting shall be determined with regard to the risk level of the relevant artificial intelligence system, the type of data, the purpose of use, the technical environment and the possible consequences of its application.

Article 14. Transparency at an Appropriate Level and Traceability

14.1. The use of artificial intelligence technologies shall be understandable, controllable and reproducible to the extent necessary for internal audit, information protection, quality verification, incident response and maintenance of public trust in the Supreme Court.

14.2. Transparency in the use of artificial intelligence technologies shall not lead to the disclosure of restricted-access information, technical vulnerabilities, official information, trade secrets of providers or information that may create risks to the security of the Supreme Court.

14.3. In the event of substantial use of artificial intelligence technologies to create a document or a substantive part thereof intended for an external addressee, the responsible employee shall ensure internal recording of such use in accordance with the procedure determined by the Head of the Supreme Court Staff or the authorised structural unit.

14.4. External notification of the use of artificial intelligence technologies shall be provided in cases stipulated by law, this Regulation or a decision of the Head of the Supreme Court Staff.

14.5. Notification of the use of artificial intelligence technologies is not required where they were used exclusively for technical tasks, including spell-checking, formatting, detecting typographical errors, preliminary translation, transcription, improving the readability of a text without changing its content, or preparing the technical structure of a document.

Article 15. Official Style and Institutional Authenticity of the Supreme Court

15.1. An employee may not mechanically transfer text generated by an artificial intelligence system into an official document without substantive, linguistic, stylistic and legal verification.

15.2. Text prepared or edited using artificial intelligence technologies shall comply with the standards of the Ukrainian literary language, official style, legal accuracy, terminological consistency, internal document-management standards of the Supreme Court, and the requirements of clarity, conciseness, impartiality, professional restraint, accessibility and non-discriminatory language.

15.3. The use in official documents of stylistic constructions, conclusions, assessments, emotionally coloured wording or templates that may create an impression of automated, unverified or inauthentic origin of a Supreme Court document shall not be permitted.

15.4. The use of artificial intelligence technologies in preparing analytical, academic, training, informational or reporting materials shall not result in plagiarism, concealed borrowing, infringement of the intellectual property rights of third parties, or uncontrolled transfer to third parties or commercial developers of artificial intelligence systems of rights to official materials or results of intellectual activity created in connection with the performance of official duties.

Section IV. Scope of Application, Permitted Areas of Use and Prohibitions

Article 16. General Conditions for Permissible Use

16.1. The use of artificial intelligence technologies by employees of the Supreme Court Staff shall be permitted only within the scope of official tasks that:

16.1.1. fall within the competence of the relevant employee or structural unit;

16.1.2. are not connected with judicial decision-making;

16.1.3. do not involve interference with the judge's inner conviction;

16.1.4. do not involve the assessment of evidence, determination of a legal position in a particular court case or forecasting of the outcome of its consideration;

16.1.5. do not involve the processing of restricted-access information in unprotected systems;

16.1.6. comply with this Regulation and other internal acts of the Supreme Court.

16.2. Publicly available artificial intelligence systems may be used exclusively for technical, reference, linguistic, training, communication, organisational or analytical tasks that do not involve the entry, uploading, transmission or other processing of restricted-access information.

16.3. An employee using a publicly available artificial intelligence system shall, before commencing work, make sure that the relevant task can be performed without disclosing restricted-access information and without the risk of identifying a particular person, court case, official document, internal position of the court or non-public procedural or organisational context.

Article 17. Permitted Areas of Use of Artificial Intelligence Technologies

17.1. Subject to compliance with this Regulation, employees of the Supreme Court Staff may use artificial intelligence technologies for the following tasks:

17.1.1. summarising open judicial practice for the purpose of ensuring its unity in accordance with the powers of the Supreme Court;

17.1.2. preliminary analysis of large volumes of open information, including legislation, public reports, international documents, academic publications, statistical data and other open sources;

17.1.3. preparation of preliminary drafts of analytical materials, memoranda, reviews, information notes, presentations, internal training materials and reports, subject to mandatory professional verification of their content by the responsible employee;

17.1.4. searching, structuring and thematic grouping of open legal positions of the Supreme Court, judicial practice, international standards, academic sources or comparative-law materials;

17.1.5. populating, technically organising and improving the search capabilities of the Database of Legal Positions of the Supreme Court, subject to prior human verification of each substantive element entered into that database;

- 17.1.6. analysing judicial decisions that are publicly available in order to identify systemic causes of disputes, prepare proposals for improving legislation, enhance judicial statistics, organise work or develop preventive justice;
- 17.1.7. preparing informational, explanatory, communication and educational materials about the activities of the Supreme Court, provided that such materials do not contain restricted-access information and do not create a false impression of the court's position in a particular case;
- 17.1.8. creating or improving materials for professional training, advanced training, self-development of employees, internal training sessions, methodological materials and test assignments;
- 17.1.9. automating repetitive technical work processes, including sorting open data, creating tables, technical structuring of information, preparing templates, charts, diagrams and visualisations;
- 17.1.10. technical improvement of texts: spell-checking, stylistic proofreading, unification of terminology, improvement of readability, structuring or shortening without changing legal content;
- 17.1.11. preliminary translation of documents from foreign languages into Ukrainian or from Ukrainian into foreign languages, subject to subsequent professional verification of the translation by the responsible employee;
- 17.1.12. preparation of draft responses, information notes or communication materials in response to requests that do not contain restricted-access information and do not concern the substance of a particular court case;
- 17.1.13. creation of chatbots or other automated reference services for navigating visitors, participants in court proceedings or users of the official electronic resources of the Supreme Court on general matters;
- 17.1.14. searching for new ideas regarding the organisation of work processes, improvement of the quality of internal communication, training, openness and accessibility of information about the activities of the Supreme Court;
- 17.1.15. other auxiliary, technical or analytical tasks that comply with this Regulation, are not connected with the administration of justice and do not create risks to judicial independence, human rights, information security or trust in the Supreme Court.

Article 18. Use of Embedded Office Artificial Intelligence Technologies

18.1. The use of low-risk embedded office artificial intelligence technologies shall not require separate approval if such tools:

- 18.1.1. do not independently generate legally significant content;
- 18.1.2. do not transfer official data to external providers without permission;
- 18.1.3. do not process restricted-access information outside the protected information environment of the Supreme Court;
- 18.1.4. do not affect the rights, obligations, assessment, liability or legal status of natural or legal persons;
- 18.1.5. are not used to analyse the behaviour, productivity or professional qualities of employees or judges.
- 18.2. Low-risk embedded office artificial intelligence technologies may include, in particular, automatic spell-checking, word autocomplete, technical formatting, detection of typographical errors, improvement of text readability, intelligent search within permitted sources or technical navigation.

Article 19. General Prohibitions

- 19.1. Employees of the Supreme Court Staff are prohibited from using any artificial intelligence systems for:
- 19.1.1. determining, forming or changing the content of judicial decisions;
- 19.1.2. automatically creating draft judgments, rulings, separate opinions of judges or other procedural documents adopted within judicial proceedings;

- 19.1.3. assessing evidence, establishing factual circumstances of a case, or forming substantive-law or procedural conclusions in a particular case;
- 19.1.4. providing recommendations on the merits of resolving a particular court dispute;
- 19.1.5. forecasting the decision of a judge, court composition or judicial panel in a particular case;
- 19.1.6. analysing the confidentiality of judicial deliberations or the internal process of forming a judge's conviction;
- 19.1.7. processing information from closed court hearings;
- 19.1.8. uploading case-file materials to publicly available artificial intelligence systems or systems not approved for that purpose;
- 19.1.9. processing personal data, official information, internal correspondence or non-public draft documents in publicly available artificial intelligence systems;
- 19.1.10. covert surveillance, assessment, ranking, profiling or forecasting of the behaviour of judges or employees;
- 19.1.11. automated adoption of personnel, disciplinary, financial or other managerial decisions concerning employees;
- 19.1.12. creating or disseminating synthetic content that imitates judges, employees, official communications or the position of the Supreme Court without lawful grounds and proper authorisation;
- 19.1.13. creating materials that may mislead as to the source, authorship, content or official position of the Supreme Court;
- 19.1.14. circumventing established rules of document management, information protection, cybersecurity, access control or internal approval of documents;
- 19.1.15. using systems whose terms provide for uncontrolled transfer of official materials, prompts, documents or the results of their processing to third parties, the use of such materials, prompts, documents or results to train commercial models, or other terms incompatible with the interests of the Supreme Court;
- 19.1.16. influencing, attempting to influence or interfering with the operation of the automated court document management system or automated allocation of court cases.

Article 20. Prohibitions Relating to Court Case Materials and Judicial Activity

- 20.1. Court case-file materials, including statements of claim, appeals and cassation complaints, applications, motions, responses, objections, explanations, evidence, expert opinions, hearing minutes, procedural documents of the parties, materials of closed court hearings and other non-public procedural information, shall not be uploaded, copied, entered as prompts or otherwise processed in publicly available artificial intelligence systems.
- 20.2. It is prohibited to use artificial intelligence technologies to prepare legal conclusions concerning a particular court case if such use may create a risk of interference in the administration of justice, substitution of judicial discretion or disclosure of restricted-access information.
- 20.3. The use of open judicial decisions for summarising practice, statistical analysis, identification of systemic problems or preparation of academic analytical materials shall be permitted only in compliance with this Regulation, personal data protection legislation, the principles of data minimisation and purpose limitation, and with anonymisation of information that allows direct or indirect identification of a natural person or a particular court case, where necessary in view of the purpose, method and environment of processing.

Article 21. Prohibitions Relating to the Monitoring of the Behaviour of Employees and Judges

21.1. The use of artificial intelligence systems for covert monitoring, surveillance, assessment of behaviour, productivity, professional qualities, psycho-emotional state, communication style or other characteristics of employees of the Supreme Court Staff or judges of the Supreme Court shall be prohibited. The prohibition shall extend, in particular, to the use of systems for automated emotion recognition, affective computing, biometric categorisation, psychological, behavioural or professional profiling of persons, except in cases expressly provided for by law.

21.2. The creation of automated ratings, assessments, forecasts or profiles of employees or judges on the basis of their documents, correspondence, writing style, activity in information systems, statistical indicators or other data shall not be permitted without a direct legal basis, proper purpose, defined procedure, safeguards against abuse and compliance with legislative requirements.

21.3. Technical logging of the use of approved artificial intelligence systems shall be permitted only for the purposes of information security, internal audit, incident response, verification of compliance with this Regulation and ensuring the proper functioning of systems. Such logging may not be used as a covert means of assessing the productivity or behaviour of employees.

Section V. Approval of Artificial Intelligence Systems, the Register and Risk Levels

Article 22. Register of Approved Artificial Intelligence Systems

22.1. In order to ensure controlled and safe use of artificial intelligence technologies in the Supreme Court Staff, a Register of Approved Artificial Intelligence Systems shall be maintained.

22.2. The Register shall be maintained by the authorised structural unit designated by the Head of the Supreme Court Staff.

22.3. The Register shall contain information on artificial intelligence systems whose use in the Supreme Court Staff is permitted within defined limits.

22.4. The Register shall include, in particular:

22.4.1. the name of the artificial intelligence system;

22.4.2. the name of the developer, provider or administrator of the system, where such information is available;

22.4.3. the type of system: publicly available, corporate, local, cloud-based, embedded or other;

22.4.4. the purpose and permitted areas of use;

22.4.5. the categories of data whose processing is permitted or prohibited;

22.4.6. the assigned risk level;

22.4.7. the main restrictions on use;

22.4.8. the responsible structural unit or official;

22.4.9. the date of entry in the Register;

22.4.10. the term of validity of approval or the date of the next review;

22.4.11. information on the results of security, legal or organisational verification;

22.4.12. decisions on suspension, restriction or termination of use of the system, where such decisions have been taken;

22.4.13. information on the model, version, configuration or other identifying characteristics of the system, where necessary to determine the approved variant of its use.

22.5. The procedure for maintaining the Register, the scope of information, the level of access to it and the responsible persons shall be determined by the Head of the Supreme Court Staff or by a structural unit authorised by him or her.

22.6. The Register shall be internal and official in nature, unless otherwise determined by the Head of the Supreme Court Staff. Publication of information on artificial intelligence systems entered in the Register shall be permitted only in a generalised scope that does not disclose restricted-access information, technical vulnerabilities, security parameters, access conditions, providers' trade secrets or other information whose disclosure may create risks for the Supreme Court.

Article 23. Risk Levels of Artificial Intelligence Systems

23.1. Artificial intelligence systems used or planned for use in the Supreme Court Staff shall be classified by risk level.

23.2. Low-risk systems may include systems or functions used for technical, linguistic, reference or training tasks and not involving the processing of restricted-access information, personal data, court case-file materials or independent generation of legally significant content.

23.3. Medium-risk systems may include systems used for preparing preliminary drafts of analytical materials, summarising open judicial practice, processing large volumes of open information, creating internal training materials, communication texts or technical organisation of open data.

23.4. High-risk systems may include systems that:

23.4.1. process or may process restricted-access information;

23.4.2. operate within critical or important information systems of the Supreme Court;

23.4.3. have a material impact on organisational, personnel, financial or other managerial processes;

23.4.4. are used for automated classification, ranking or analytical processing of data, the consequences of which may affect the rights, interests or legal status of persons;

23.4.5. create heightened risks to information security, confidentiality, judicial independence or trust in the Supreme Court.

23.5. High-risk systems may be used only after a prior legal, organisational and security assessment and a human rights impact assessment, entry in the Register, and determination of special conditions for their use.

23.6. It shall be prohibited to use an artificial intelligence system where its risk level, data processing conditions, training sources, third-party access, data storage location or legal consequences of use cannot be established to a degree sufficient for safe official application.

23.7. Irrespective of the assigned risk level, the use of artificial intelligence systems for the purposes provided for in Articles 7, 19, 20 and 21 of this Regulation shall be prohibited. The classification of a system as low-, medium- or high-risk shall not legalise any type of use of artificial intelligence technologies prohibited by this Regulation.

Article 24. Approval of Artificial Intelligence Systems

24.1. The use of corporate, local, cloud-based, integrated or other artificial intelligence systems for official tasks, except for the use of publicly available systems for low-risk tasks, shall take place after their approval in accordance with the procedure established by this Regulation and decisions of the Head of the Supreme Court Staff.

24.2. Before an artificial intelligence system is approved, the following shall be assessed:

24.2.1. the purpose of using the system;

- 24.2.2. the functional capabilities of the system;
 - 24.2.3. the categories of data intended to be processed;
 - 24.2.4. the legal regime for processing, storing and transferring data;
 - 24.2.5. the possibility of using input data for training or improving models;
 - 24.2.6. access of the provider or third parties to input data and outputs of the system;
 - 24.2.7. the location of data storage, where such information is available;
 - 24.2.8. the terms of the licence, contract or rules of use;
 - 24.2.9. cybersecurity, access control, authentication and logging measures;
 - 24.2.10. possible risks of errors, hallucinations, bias, unauthorised access, harmful influence on outputs or data leakage;
 - 24.2.11. the possibility of suspending or terminating use of the system;
 - 24.2.12. compliance of the system with the requirements of this Regulation;
 - 24.2.13. compliance of the system with relevant ethical standards for the responsible use of artificial intelligence technologies in the field of justice, including the principles of respect for human rights, non-discrimination, human oversight, safety, transparency at an appropriate level and explainability to the extent necessary and possible in view of the purpose and technical characteristics of the system;
 - 24.2.14. for high-risk systems, the results of a prior human rights impact assessment conducted to an extent proportionate to the purpose, functional capabilities and risk level of the system, taking into account relevant Council of Europe methodologies for assessing the impact of artificial intelligence systems on human rights, democracy and the rule of law.
- 24.3. Following the assessment of an artificial intelligence system, one of the following decisions may be taken:
- 24.3.1. to permit use of the system without additional restrictions within defined limits;
 - 24.3.2. to permit use of the system with restrictions;
 - 24.3.3. to permit pilot use of the system for a defined period;
 - 24.3.4. to refuse use of the system;
 - 24.3.5. to suspend or terminate use of the system.
- 24.4. Approval of an artificial intelligence system shall not release employees from the obligation to comply with this Regulation, use the system only within the defined purpose, permitted functions and categories of data, verify its outputs and ensure information protection.
- 24.5. A material change in the functional capabilities of an approved artificial intelligence system, the underlying model, the conditions for processing or storing data, the circle of users, the categories of data, the technical infrastructure or the risk level shall constitute grounds for reassessment and review of the approval conditions. Until such assessment is completed, use of the modified system may be restricted or suspended.

Section VI. Procedure for the Use of Artificial Intelligence Technologies

Article 25. General Duties of an Employee

- 25.1. Before using artificial intelligence technologies, an employee shall:
- 25.1.1. determine the official purpose of use;
 - 25.1.2. verify whether such use is permitted by this Regulation;

- 25.1.3. ascertain whether the task involves the entry of restricted-access information;
- 25.1.4. assess the risk of identifying a particular person, court case, official document or internal position of the Supreme Court;
- 25.1.5. where necessary, seek clarification from the immediate supervisor or the authorised structural unit;
- 25.1.6. use only approved artificial intelligence systems entered in the Register, except where embedded office technologies and publicly available systems are used to perform low-risk technical, auxiliary, linguistic or training tasks defined by this Regulation, without entering restricted-access information or other official data.
- 25.2. When using artificial intelligence technologies, an employee shall:
 - 25.2.1. formulate prompts clearly, correctly, in anonymised form and to the minimum extent necessary;
 - 25.2.2. refrain from entering information whose processing is prohibited by this Regulation;
 - 25.2.3. critically assess the outputs obtained;
 - 25.2.4. verify facts, sources, quotations, particulars, dates, legal conclusions and translations;
 - 25.2.5. refrain from using unverified information as reliable;
 - 25.2.6. record substantial use of artificial intelligence technologies in cases defined by this Regulation or decisions of the Head of the Supreme Court Staff;
 - 25.2.7. report incidents or suspected incidents in accordance with the established procedure.

Article 26. Rules for Formulating Prompts

- 26.1. A prompt to an artificial intelligence system shall be formulated so as not to disclose restricted-access information and not to create a risk of identifying a particular person, court case, internal document or official discussion.
- 26.2. Prompts to publicly available artificial intelligence systems shall not include:
 - 26.2.1. surnames, first names or patronymics of persons, unless such data are open and officially permissible for use;
 - 26.2.2. numbers of court cases, proceedings, documents or internal registration records;
 - 26.2.3. addresses, telephone numbers, email addresses, registration numbers, bank details or other identifiers;
 - 26.2.4. non-public circumstances of a court case;
 - 26.2.5. fragments of court case-file materials;
 - 26.2.6. fragments of internal official correspondence;
 - 26.2.7. drafts of judicial decisions, procedural documents or internal analytical documents that are not publicly available;
 - 26.2.8. any combinations of information that, taken together, may allow identification of a particular case, person or official context.
- 26.3. Prompts shall be clear, neutral, correct and directed towards obtaining assistance in the form of structuring, summarising open information, linguistic editing, technical processing or preliminary analytical support. It shall not be permitted to formulate prompts in a manner that contains leading, manipulative, discriminatory or evaluative assumptions, may cause distortion of the output, or shifts responsibility for the content of an official document to an artificial intelligence system.

Article 27. Verification of Outputs of Artificial Intelligence Systems

27.1. Outputs of artificial intelligence systems shall not have independent evidentiary, normative, official or legal force.

27.2. Before using an output of an artificial intelligence system in official activity, an employee shall verify:

27.2.1. the factual accuracy of the information;

27.2.2. the existence and reliability of sources;

27.2.3. the accuracy of quotations;

27.2.4. the validity of legal acts;

27.2.5. the current relevance of judicial practice;

27.2.6. the correctness of translation;

27.2.7. the absence of fabricated particulars, non-existent sources or distorted conclusions;

27.2.8. the conformity of the output with the official purpose, official style and standards of the Supreme Court.

27.3. Use of the outputs of an artificial intelligence system without verification against primary sources shall not be permitted where the relevant output contains factual statements, legal conclusions, particulars, quotations, statistical data or references to sources.

27.4. Where errors, hallucinations, distortions of content, unreliable sources or signs of bias are identified, the employee shall refuse to use the relevant output or use it only after complete correction and verification.

27.5. An employee of the Staff who provides a judge or the head of a structural unit with analytical memoranda, reviews of judicial practice, information materials or draft responses prepared with substantial auxiliary use of artificial intelligence technologies shall ensure internal confirmation of the fact of his or her personal factual, normative, linguistic and substantive verification of such materials against official or other reliable primary sources in accordance with the procedure determined by the Head of the Supreme Court Staff or the authorised structural unit.

27.6. Where an analytical memorandum, review of judicial practice, selection of sources or other informational and analytical material is prepared for a judge or a judicial panel with substantial use of artificial intelligence technologies, the responsible employee shall inform the addressee of that fact in the manner determined by the Head of the Supreme Court Staff or the authorised structural unit. Such notification shall not release the employee from the obligation to independently verify the material and may not be interpreted as shifting responsibility for its content to the addressee.

Article 28. Use of Artificial Intelligence Technologies for Translation

28.1. Artificial intelligence technologies may be used for preliminary translation of texts where this is not connected with the processing of restricted-access information in publicly available or unapproved systems.

28.2. A translation obtained through an artificial intelligence system shall be subject to professional verification by the employee who uses such translation in official activity.

28.3. Where a translation concerns legal concepts, international instruments, judicial practice, procedural documents or official communication, the employee shall verify the conformity of the translation with the content of the original, legal terminology, official texts of international instruments, official translations, relevant legal glossaries and the context of the relevant document. A translation obtained using artificial intelligence technologies may not replace professional translation in cases where such translation is required by law, the nature of the document or a decision of an authorised official.

28.4. Machine or automated translation may not be submitted as a final official text without proper professional verification.

Article 29. Use of Artificial Intelligence Technologies in External Communication

29.1. Artificial intelligence technologies may be used to prepare preliminary drafts of communication, informational, educational or explanatory materials about the activities of the Supreme Court, provided that such materials:

29.1.1. do not contain restricted-access information;

29.1.2. do not concern the substance of a particular court case where such communication may be perceived as the court's position on the case;

29.1.3. do not create a false impression of the official position of the Supreme Court;

29.1.4. undergo proper substantive, legal, linguistic and communication review by responsible employees.

29.2. It shall be prohibited to disseminate, on behalf of the Supreme Court, materials created or materially altered using artificial intelligence technologies where they may mislead as to the authorship, source, content, time, circumstances or official nature of the communication.

29.3. Synthetic audio, video, photographic or other content that imitates judges, employees, official symbols, speeches or communications of the Supreme Court may be used only in exceptional cases where there is a lawful purpose, proper authorisation, clear labelling and safeguards against misleading persons. Where technically possible, such content shall be accompanied by machine-readable labelling of its artificial origin and by a clearly perceptible disclosure to natural persons.

Article 30. Chatbots and Automated Reference Services

30.1. Chatbots and other automated services created or used with the application of artificial intelligence technologies may be used by the Supreme Court to provide reference, navigation, informational or educational support to users.

30.2. Such services may not:

30.2.1. provide legal advice concerning a particular court case;

30.2.2. forecast the outcome of a case;

30.2.3. interpret a person's procedural rights or obligations as the final position of the court;

30.2.4. process restricted-access information without a proper legal basis and protected environment;

30.2.5. create the impression of communication with a judge or authorised employee of the Supreme Court where this is not true.

30.3. Users of automated reference services shall be informed that they are interacting with an automated tool and that the information provided by it is for reference purposes, unless otherwise expressly established by law or by an official decision of the Supreme Court.

30.4. A user of an automated reference service shall be provided with a clear opportunity to contact an authorised employee of the Supreme Court on matters that fall outside the reference function of such service.

Section VII. Data Protection, External Systems and Cybersecurity

Article 31. Restrictions on External Artificial Intelligence Systems

31.1. When using external artificial intelligence systems, an employee shall, to the extent technically possible, select settings that prohibit the use of input data, prompts, documents or text fragments for the training, additional training, testing, evaluation or improvement of models of the developer or third parties.

31.2. The use of external artificial intelligence systems for official tasks shall be prohibited where their terms of use provide for:

31.2.1. alienation of proprietary rights to official material, the granting to the provider or third parties of unjustifiably broad rights to use such material, or other terms not necessary for the provision of the relevant service;

31.2.2. use of official material for training or improving commercial models without proper authorisation of the Supreme Court;

31.2.3. uncontrolled transfer of data to third parties;

31.2.4. an undefined or non-transparent procedure for storing, processing or deleting data;

31.2.5. other terms incompatible with the requirements of confidentiality, information protection, intellectual property and the interests of the Supreme Court.

31.3. If it is impossible to establish the terms of use of an artificial intelligence system, the legal regime of data processing, the location of data storage, the possibility of using input data, prompts, documents or the results of their processing for training models, or the procedure for third-party access to such data, the use of that system for official tasks shall be prohibited until the relevant verification has been carried out.

31.4. When concluding contracts, licensing agreements or other legal instruments concerning the use of corporate, cloud-based or integrated artificial intelligence systems, the Supreme Court shall, where possible and taking into account the risk level of the system, provide for conditions prohibiting the use of input data, prompts, documents or the results of their processing for training or improving models, minimising retention periods for prompts and outputs, restricting logging, temporary storage of data and third-party access, and deleting or returning data after their processing has been completed. For systems that may process restricted-access information, priority shall be given to solutions with a zero- or minimal-data-retention policy.

Article 32. Processing of Restricted-Access Information

32.1. Processing restricted-access information using artificial intelligence technologies shall be permitted only where such processing:

32.1.1. is expressly permitted by law and internal acts of the Supreme Court;

32.1.2. is carried out within the protected information environment of the Supreme Court or in another approved environment with proper security guarantees;

32.1.3. is necessary for the performance of a specific official task;

32.1.4. complies with the principles of proportionality, data minimisation and purpose limitation;

32.1.5. is carried out with appropriate access control, logging and other information security measures.

32.2. Processing restricted-access information in publicly available artificial intelligence systems shall be prohibited.

32.3. Before using an artificial intelligence system to work with restricted-access information, the following shall be determined:

32.3.1. the legal basis for processing;

32.3.2. the categories of information to be processed;

32.3.3. the circle of persons who have access to the system;

32.3.4. technical and organisational protection measures;

32.3.5. the procedure for storage, deletion, backup and recovery of data;

32.3.6. the procedure for responding to possible incidents.

Article 33. Cybersecurity Requirements

33.1. When implementing and using artificial intelligence systems, specific cybersecurity threats shall be taken into account and minimised, including unauthorised access, data leakage, malicious software impact, formulation of harmful or manipulative prompts aimed at bypassing the system's security restrictions, intentional modification or distortion of sources or datasets, substitution of outputs, unauthorised generation of synthetic content, and risks of disclosure of official information through prompts, outputs, event logs or system feedback channels.

33.2. For medium- and high-risk systems, where necessary, the following shall be defined:

33.2.1. the procedure for user authentication;

33.2.2. rules of access to the system;

33.2.3. logging of user actions;

33.2.4. restrictions on data entry and uploading;

33.2.5. the procedure for storage, deletion, backup and recovery of data;

33.2.6. measures to protect against unauthorised access;

33.2.7. the procedure for checking updates, integrations and external components;

33.2.8. the procedure for responding to errors, failures, suspicious outputs or incidents.

33.3. Where critical technical, legal or security risks are identified, use of the artificial intelligence system shall be suspended until verification is completed and a decision is taken on further use, restriction of use or exclusion of that system from the Register.

Section VIII. Monitoring, Audit, Incidents and Liability

Article 34. Monitoring the Use of Artificial Intelligence Technologies

34.1. The leadership of the Supreme Court Staff may initiate monitoring of the use of artificial intelligence technologies within the Supreme Court Staff for the purpose of ensuring compliance with this Regulation, protecting information, assessing effectiveness, identifying risks and preventing incidents.

34.2. Monitoring shall be carried out in a manner that complies with Ukrainian legislation, internal acts of the Supreme Court, and the principles of proportionality, transparency at an appropriate level, data minimisation and respect for the rights of employees.

34.3. Monitoring may not be used as a means of covert surveillance, unjustified profiling, or assessment of the behaviour, productivity or professional qualities of employees or judges.

34.4. Monitoring results may be used for:

34.4.1. improving the rules for using artificial intelligence technologies;

34.4.2. updating the Register;

34.4.3. preparing training measures;

34.4.4. eliminating identified risks;

34.4.5. responding to incidents;

34.4.6. preparing generalised information on the implementation of artificial intelligence technologies.

34.5. Employees shall be informed of the general rules for monitoring and logging the use of approved artificial intelligence systems, including the purpose of such monitoring, the types of data that may be recorded, the periods for their storage, the circle of persons who have access to the relevant information, and safeguards against the use of monitoring as a covert means of assessing employees' behaviour or productivity.

Article 35. Internal Audit

35.1. The use of artificial intelligence systems in the Supreme Court Staff may be subject to internal audit.

35.2. Internal audit may cover:

35.2.1. compliance of the use of artificial intelligence systems with this Regulation;

35.2.2. proper maintenance of the Register;

35.2.3. compliance with permitted limits of use;

35.2.4. effectiveness of information protection measures;

35.2.5. quality of verification of outputs of artificial intelligence systems;

35.2.6. compliance with requirements concerning transparency, recording and logging;

35.2.7. the state of incident response;

35.2.8. the need to update this Regulation or internal procedures.

35.3. Based on the results of internal audit, recommendations may be prepared regarding restriction, suspension, termination or expansion of the use of particular artificial intelligence systems, as well as additional training of employees.

Article 36. Incidents Related to the Use of Artificial Intelligence

36.1. An employee shall immediately notify his or her immediate supervisor or the authorised structural unit of an incident or a justified suspicion of an incident related to the use of artificial intelligence technologies.

36.2. Incidents shall include, in particular:

36.2.1. entering restricted-access information into a publicly available or unapproved artificial intelligence system;

36.2.2. suspicion of leakage, unlawful storage or transfer of data to third parties;

36.2.3. use of an unreliable, fabricated or unverified output in an official document;

36.2.4. identification of a systemic error, bias or erroneous output that may affect the rights of persons, the interests of justice or trust in the Supreme Court;

36.2.5. unauthorised use of an artificial intelligence system for prohibited purposes;

36.2.6. creation or dissemination of synthetic content that may mislead;

36.2.7. violation of rules on access, logging, information protection or internal approval;

36.2.8. another event that may create a material risk to the security of the Supreme Court, human rights, judicial independence or public trust.

36.3. In the event of an incident or suspected incident, the following initial measures may be applied:

36.3.1. termination or suspension of use of the relevant system;

36.3.2. restriction of access to the system;

36.3.3. recording the circumstances of the incident;

36.3.4. assessment of possible data leakage or unlawful processing;

36.3.5. notification of responsible structural units;

36.3.6. removal of unreliable information from an official document or its correction;

36.3.7. conducting additional verification, training or instruction;

36.3.8. adoption of a decision to change the conditions of use, suspend or terminate use of the relevant system.

Article 37. Liability of Employees

37.1. An employee shall be liable for compliance with this Regulation when using artificial intelligence technologies.

37.2. Violation of this Regulation may constitute grounds for applying disciplinary or other liability measures in accordance with Ukrainian legislation and internal acts of the Supreme Court.

37.3. When deciding on liability, consideration shall be given to the nature of the violation, its consequences, the existence of harm or risk of harm, the form of fault, the employee's official duties, the fact of reporting an incident, measures taken to remedy the consequences and the employee's previous practice of compliance with information security requirements.

37.4. Good-faith reporting by an employee of an incident or error related to the use of artificial intelligence technologies shall be taken into account when assessing his or her actions and determining further response measures.

Section IX. Training, Openness, Review and Final Provisions

Article 38. Training of Employees

38.1. Employees of the Supreme Court Staff who use or may use artificial intelligence technologies in official activity shall undergo periodic training or instruction on the responsible use of such technologies.

38.2. Training shall cover, in particular:

38.2.1. the requirements of this Regulation;

38.2.2. the capabilities, limitations and main risks of generative artificial intelligence systems;

38.2.3. rules for formulating safe prompts;

38.2.4. rules of anonymisation, data minimisation and protection of restricted-access information;

38.2.5. methods for identifying hallucinations, factual errors and algorithmic bias;

38.2.6. verification of outputs against official or other reliable primary sources;

38.2.7. rules of safe behaviour in the digital environment when using artificial intelligence systems;

38.2.8. the procedure for reporting and responding to incidents;

38.2.9. ethical and communication aspects of the use of artificial intelligence technologies in the activities of the Supreme Court.

38.3. Employees shall be familiarised with this Regulation in accordance with the procedure determined by the Head of the Supreme Court Staff.

38.4. Completion by employees of training or instruction on the responsible use of artificial intelligence technologies shall be recorded in accordance with the procedure determined by the Head of the Supreme Court Staff or the authorised structural unit.

Article 39. Openness and Public Trust

39.1. The Supreme Court supports an open, responsible and human-rights-oriented approach to the use of artificial intelligence technologies in judicial administration.

39.2. Generalised information on the areas of use of artificial intelligence technologies, results, effectiveness, risks and security measures may be published on the official website of the Supreme Court or in other forms of public communication.

39.3. Publication of such information shall not disclose restricted-access information, personal data, technical vulnerabilities, internal security procedures or information that may create risks for the Supreme Court, judges, employees or participants in court proceedings.

39.4. This Regulation may be the subject of professional discussion with academics, representatives of the judiciary, and experts in law, information security, personal data protection, ethics and responsible use of artificial intelligence technologies.

39.5. Based on monitoring, audit and analysis of the practice of using artificial intelligence technologies in the Supreme Court Staff, a generalised internal report may be prepared containing information on the areas of use of such technologies, approved systems, identified risks, safeguards adopted, training conducted, a generalised description of incidents without disclosure of restricted-access information, and proposals for updating this Regulation, internal procedures or training programmes.

Article 40. Review and Updating of the Regulation

40.1. This Regulation shall be subject to periodic review, taking into account the development of artificial intelligence technologies, changes in Ukrainian legislation, international standards, judicial practice, the practice of the Supreme Court and the results of internal monitoring and audit.

40.2. Review of this Regulation may be initiated by the Head of the Supreme Court Staff, the authorised structural unit, or following the identification of material risks, incidents or the need to clarify rules on the use of artificial intelligence technologies.

40.3. Following a review, amendments to this Regulation, additional instructions, methodological recommendations, model safe prompts, checklists, forms for internal recording of the use of artificial intelligence technologies or other auxiliary documents may be prepared.

40.4. When reviewing this Regulation and updating the Register of Approved Artificial Intelligence Systems, the authorised structural unit shall take into account official documents, tools, analytical materials and recommendations of the Council of Europe, CEPEJ, its advisory and working bodies on artificial intelligence and cyberjustice, the European Union, UNESCO, national authorities in the fields of digital transformation, cybersecurity and personal data protection, as well as the practical experience of the Supreme Court in the safe and responsible use of artificial intelligence technologies. In particular, account may be taken of the CEPEJ European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, the Council of Europe HUDERIA methodology, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and other relevant documents in this field.

Article 41. Final Provisions

41.1. This Regulation shall enter into force on the date of its approval, unless otherwise determined by an order of the Head of the Supreme Court Staff.

41.2. Heads of independent structural units of the Supreme Court Staff shall ensure that employees are familiarised with this Regulation and shall facilitate its proper implementation.

41.3. The authorised structural unit shall provide methodological support for the application of this Regulation, prepare clarifications, maintain the Register of Approved Artificial Intelligence Systems and coordinate monitoring, audit and incident response measures.

41.4. Matters not regulated by this Regulation shall be resolved in accordance with the Constitution of Ukraine, the laws of Ukraine, acts of the Supreme Court and decisions of the Head of the Supreme Court Staff.

41.5. If the provisions of a contract, licence terms, rules of use or technical documentation of an artificial intelligence system conflict with the requirements of this Regulation or create unacceptable risks for the Supreme Court, such system may not be used in official activity until the relevant conflicts or risks have been eliminated.

41.6. The use of artificial intelligence technologies in the activities of the Supreme Court Staff shall be carried out in a manner that combines openness to innovation with the unconditional priority of the rule of law, judicial independence, protection of human rights and freedoms, information security and trust in the judiciary.

41.7. Within the period specified by an order of the Head of the Supreme Court Staff, the authorised structural unit shall ensure an inventory of artificial intelligence systems actually used in the Supreme Court Staff on the date this Regulation enters into force, their assessment and entry in the Register, or the preparation of proposals to restrict or terminate their use. Until such measures are completed, only embedded office technologies and publicly available artificial intelligence systems may be used for low-risk tasks without processing restricted-access information.

Material files

[Original author file](#)