1. What are some prohibited artificial intelligence practices outlined in Article 5?

Article 5 prohibits various AI practices including those using subliminal techniques, exploiting vulnerabilities based on age or disability, and categorizing individuals based on sensitive biometric data.

1. What is the objective behind prohibiting the use of AI systems deploying subliminal techniques?

The objective is to prevent AI systems from materially distorting individuals' behavior or impairing their ability to make informed decisions through deceptive techniques.

1. How does Article 5 address the exploitation of vulnerabilities of certain groups by AI systems?

It prohibits the use of AI systems exploiting vulnerabilities based on age, disability, or specific social or economic situations to distort behavior and cause significant harm.

1. What specific practice regarding biometric data categorization is prohibited?

The article prohibits the use of biometric categorization systems to deduce sensitive personal information such as race, political opinions, or sexual orientation, except for specific law enforcement purposes.

1. Under what circumstances does Article 5 prohibit the use of AI systems for evaluating or classifying individuals based on social behavior?

It prohibits such use if it leads to unjustified or disproportionate treatment in unrelated social contexts or if it unfairly penalizes individuals based on inferred or predicted characteristics.

1. When is the use of 'real-time' remote biometric identification systems in public spaces for law enforcement permitted?

It is permitted strictly for specific objectives such as targeted searches for victims or to prevent imminent threats, subject to necessary safeguards and proportionality assessments.

1. How does Article 5 regulate the use of AI systems for making risk assessments of individuals regarding criminal activities?

It prohibits the use of AI systems for risk assessments solely based on profiling or personality traits, except when supporting human assessment based on objective facts.

1. What practice related to facial recognition databases is prohibited?

The article prohibits the creation or expansion of facial recognition databases through untargeted scraping of images from the internet or CCTV footage.

1. In which contexts does Article 5 restrict the inference of emotions using AI systems?

It restricts the inference of emotions in workplace and educational institutions, except for medical or safety reasons.

1. What factors must be considered when deploying 'real-time' remote biometric identification systems in public spaces for law enforcement?

Factors include the seriousness and probability of harm, as well as the impact on rights and freedoms, with compliance to necessary safeguards and national legislation.

1. Who grants authorization for the use of 'real-time' remote biometric identification systems for law enforcement purposes?

Authorization is granted by a judicial or independent administrative authority based on a reasoned request, ensuring necessity and proportionality.

1. How does Article 5 ensure oversight and accountability for the use of such biometric identification systems?

It mandates prior authorization by judicial or administrative authorities, submission of notifications to relevant authorities, and annual reporting to the Commission.

1. What role do Member States play in regulating the use of 'real-time' remote biometric identification systems?

Member States establish detailed rules for authorization, supervision, and reporting, and may introduce more restrictive laws in accordance with Union law.

1. What information do national authorities provide to the Commission regarding the use of biometric identification systems?

They submit annual reports including the number of authorization requests, decisions, and results, facilitating Commission's publication of aggregated data on system usage.

1. What type of information is excluded from the annual reports published by the Commission?

Sensitive operational data related to law enforcement activities is excluded from the reports, ensuring privacy and security.

1. What obligations do providers of general purpose AI models have under Article 52c?

Providers are required to maintain technical documentation, share information with AI system providers, respect copyright laws, and provide a summary of training content.

1. Are there exceptions to these obligations?

Yes, providers of AI models accessible under a free and open license are exempt, except those posing systemic risks.

1. What role do providers have in cooperating with regulatory authorities?

Providers must cooperate with the Commission and national authorities as required by the regulation.

1. Can providers demonstrate compliance through codes of practice?

Yes, they can rely on codes of practice until harmonized standards are established, ensuring compliance or demonstrating alternative means for approval.

1. How will compliance be facilitated regarding technical documentation?

The Commission may adopt delegated acts to detail measurement and calculation methodologies, ensuring comparable and verifiable documentation.

1. What authority does the Commission have regarding amendments to Annexes IXa and IXb?

The Commission is empowered to adopt delegated acts to amend these annexes in response to evolving technological developments.

1. How is confidential information handled under Article 52c?

Information obtained under this article, including trade secrets, must be treated confidentially in accordance with specified obligations.

1. What is the significance of adhering to the obligations outlined in Article 52c?

Adherence to these obligations ensures transparency, accountability, and responsible usage of general purpose AI models, fostering trust and compliance with regulatory standards.

1. What is the duration of the Commission's power to adopt delegated acts under Article 73?

The Commission's power lasts for five years from the entry into force of the Regulation, with the possibility of tacit extension.

1. How does the Commission report on the delegation of power?

The Commission must submit a report nine months before the end of the five-year period, detailing the delegation of power and any proposed extension.

1. Can the European Parliament or the Council oppose the extension of the delegation of power?

Yes, either body can oppose the extension of the delegation of power, provided they do so at least three months before the end of each period.

1. How can the delegation of power be revoked?

The European Parliament or the Council can revoke the delegation of power at any time, which takes effect upon publication in the Official Journal of the European Union.

1. What happens to delegated acts if the delegation of power is revoked?

The revocation does not affect the validity of any delegated acts already in force.

1. What is the procedure for notifying the adoption of delegated acts?

The Commission must notify the European Parliament and the Council simultaneously upon adopting a delegated act.

1. When do delegated acts enter into force?

Delegated acts enter into force unless objections are raised by either the European Parliament or the Council within three months of notification, with the possibility of extension by an additional three months.

1. What information is required in the transparency information for providers of general-purpose AI models?

The transparency information should include a general description of the AI model's tasks, acceptable use policies, distribution methods, compatibility with hardware or software, software versions, architecture, input/output modalities, and licensing details.

1. What details about the model's development process should be included?

The transparency information should describe the technical means necessary for integration, input/output modalities and formats, maximum sizes, and information on the training, testing, and validation data used, including type, provenance, and curation methodologies.

1. What are the intended tasks and compatible AI systems for the general-purpose AI model?

The transparency information should specify the tasks the model is designed for, the types of AI systems it can be integrated into, and any acceptable use policies that apply.

1. How is the distribution of the general-purpose AI model documented?

The transparency information should provide details about the model's release date, methods of distribution, and any interactions with external hardware or software.

1. What licensing information is required for the general-purpose AI model?

The transparency information should include details about the model's license, ensuring downstream providers are aware of any usage restrictions or permissions.

1. What is the purpose of AI regulatory sandboxes as outlined in Article 53?

AI regulatory sandboxes aim to foster innovation, facilitate the development and testing of AI systems, and improve legal certainty for compliance with regulations.

1. When must Member States establish AI regulatory sandboxes?

Member States must establish at least one AI regulatory sandbox within 24 months after the Regulation's entry into force.

1. Can AI regulatory sandboxes be established jointly with other Member States' competent authorities?

Yes, AI regulatory sandboxes can be established jointly with one or several other Member States' competent authorities to enhance collaboration and effectiveness.

1. What role can the European Data Protection Supervisor (EDPS) play in AI regulatory sandboxes?

The EDPS may establish an AI regulatory sandbox for EU institutions, bodies, and agencies, exercising roles and tasks of national competent authorities.

1. How are resources allocated for the establishment and operation of AI regulatory sandboxes?

Competent authorities must allocate sufficient resources to comply effectively and timely with the establishment and operation of AI regulatory sandboxes, ensuring cooperation with other relevant authorities.

1. What are the objectives of AI regulatory sandboxes?

The objectives include improving legal certainty, sharing best practices, fostering innovation and competitiveness, contributing to evidence-based regulatory learning, and facilitating access to the Union market for AI systems, especially for SMEs and start-ups.

1. How are data protection and other national authorities involved in AI regulatory sandboxes?

National competent authorities ensure involvement of national data protection authorities and other relevant authorities in supervising aspects related to data processing and other national legislation.

1. What happens if significant risks to health, safety, or fundamental rights are identified during sandbox testing?

National competent authorities have the power to suspend testing temporarily or permanently if effective mitigation is not possible, ensuring protection of rights and safety.

1. What liability do providers have during experimentation in AI regulatory sandboxes?

Providers remain liable for damages, but administrative fines are not imposed if providers adhere to sandbox plans and guidance provided in good faith.

1. How do AI regulatory sandboxes facilitate cross-border cooperation?

Sandboxes are designed to support cross-border cooperation between national competent authorities, ensuring consistent practices across the Union.

1. What reporting requirements exist for national competent authorities regarding AI regulatory sandboxes?

National competent authorities submit annual reports to the AI Office and the Board, detailing progress, results, incidents, lessons learned, and recommendations.

1. How does the Commission facilitate stakeholder interaction with regulatory sandboxes?

The Commission develops a dedicated interface containing relevant information related to sandboxes, allowing stakeholders to interact and seek guidance on conformity.

1. What principles are outlined in implementing acts for the establishment and operation of AI regulatory sandboxes?

Implementing acts detail principles for eligibility and selection, application procedures, terms and conditions, accessibility, flexibility, and coordination among national competent authorities.

1. How are SMEs and start-ups supported in AI regulatory sandboxes?

SMEs and start-ups have access to free participation in sandboxes, along with assistance in fulfilling regulatory obligations and access to additional services and facilities.

1. What tools and infrastructure are developed within sandboxes to facilitate regulatory learning?

Sandboxes facilitate the development of tools and infrastructure for testing, benchmarking, assessing, and explaining dimensions of AI systems relevant for regulatory learning, such as accuracy, robustness, and cybersecurity.

1. Under what conditions can personal data be processed for developing AI systems in the AI regulatory sandbox?

Personal data can be processed if the AI systems are developed for substantial public interest, data processing is necessary, effective monitoring mechanisms are in place, and strict data protection measures are followed.

1. What are examples of areas where AI systems can be developed for substantial public interest?

Examples include public safety, public health, environmental protection, energy sustainability, transport systems, public administration efficiency, and quality of public services.

1. What requirements must be met for processing personal data in the sandbox?

The data processed must be necessary, monitored for risks to data subjects' rights, processed in a secure environment, and protected by appropriate technical measures.

1. Can personal data collected in the sandbox be shared outside of it?

No, personal data created in the sandbox cannot be shared outside of it, and sharing of originally collected data must comply with EU data protection law.

1. How are the rights of data subjects protected during the processing of personal data in the sandbox?

Processing must not lead to measures or decisions affecting data subjects, and their rights under Union law on data protection are not affected.

1. What happens to personal data once participation in the sandbox ends?

Personal data must be deleted once participation in the sandbox ends or when it reaches the end of its retention period.

1. What documentation must be kept regarding the training, testing, and validation of AI systems in the sandbox?

A complete and detailed description of the process and rationale behind the training, testing, and validation must be kept as part of the technical documentation.

1. Where should information about AI projects developed in the sandbox be published?

A short summary of AI projects, objectives, and expected results should be published on the website of the competent authorities, excluding sensitive operational data related to law enforcement activities.

1. What conditions apply to the processing of personal data for prevention or investigation of criminal offences?

Processing for criminal investigation purposes must be based on specific Member State or Union law and subject to the same conditions as other processing in the sandbox.

1. Are there any exceptions to the processing of personal data in the sandbox?

Union or Member States legislation may exclude processing for purposes other than those explicitly mentioned, and processing must comply with Union law on the protection of personal data.

1. What is required for high-risk AI systems to comply with the regulations?

High-risk AI systems must comply with the requirements outlined in the chapter, considering their intended purpose and the current state of AI technology, with consideration given to the risk management system detailed in Article 9.

1. Who is responsible for ensuring compliance of products containing AI systems?

Providers of products containing AI systems are responsible for ensuring full compliance with all applicable requirements under both this Regulation and Union harmonization legislation listed in Annex II, Section A.

1. How can providers ensure compliance of high-risk AI systems with the regulations?

Providers have the option to integrate necessary testing, reporting processes, information, and documentation into existing documentation and procedures required under Union harmonization legislation, aiming to ensure consistency, avoid duplication, and minimize additional burdens.

1. What factors should providers consider when integrating compliance processes?

Providers should consider the requirements outlined in Chapter 2 of the Regulation, ensuring alignment with existing documentation and procedures under Union harmonization legislation, while also striving for consistency and avoiding unnecessary duplication.

1. What is the purpose of allowing providers to integrate compliance processes?

Allowing integration of compliance processes aims to streamline procedures, reduce administrative burden, and ensure consistency in compliance efforts for products containing AI systems, thus facilitating adherence to regulatory requirements.

1. What transparency requirements apply to high-risk AI systems?

High-risk AI systems must be designed and developed to ensure sufficient transparency in their operation, enabling deployers to interpret the system's output appropriately to achieve compliance with relevant obligations.

1. What information must be provided with high-risk AI systems?

High-risk AI systems must be accompanied by instructions for use containing concise, complete, correct, and clear information relevant to users, ensuring accessibility and comprehensibility.

1. What details must the instructions for use include?

The instructions for use must include information such as the provider's identity and contact details, characteristics and limitations of the AI system's performance, including its intended purpose, accuracy metrics, robustness, and cybersecurity.

1. What circumstances regarding the AI system's use should be disclosed?

The instructions should disclose any known or foreseeable circumstances that may pose risks to health, safety, or fundamental rights, considering both intended use and reasonably foreseeable misuse.

1. What specifications regarding input data should be provided?

Specifications for input data, training, validation, and testing datasets used should be included, considering the AI system's intended purpose.

1. What information should be provided to facilitate the interpretation of the AI system's output?

Information to enable deployers to interpret the system's output appropriately should be included, especially when relevant to the system's intended use.

1. What changes to the AI system's performance should be disclosed?

Changes predetermined by the provider at the initial conformity assessment should be disclosed, if any.

1. What human oversight measures must be described?

The instructions should describe human oversight measures, including technical measures to facilitate the interpretation of AI system outputs by deployers.

1. What computational and hardware resources information should be included?

Information regarding computational and hardware resources needed, expected lifetime, maintenance, care measures, and software updates should be provided.

1. What mechanisms related to log collection and interpretation should be described?

The instructions should include a description of mechanisms within the AI system allowing users to collect, store, and interpret logs in accordance with relevant regulations.

1. What is the purpose of human oversight in high-risk AI systems?

Human oversight aims to prevent or minimize risks to health, safety, or fundamental rights during the AI system's use, particularly when risks persist despite other regulatory requirements.

1. What requirements must high-risk AI systems meet regarding human oversight?

High-risk AI systems must be designed to allow effective oversight by natural persons during their use, with appropriate human-machine interface tools.

1. How should oversight measures be tailored to the AI system?

Oversight measures must be commensurate with the risks, level of autonomy, and context of use, and can be built into the system by the provider or identified for implementation by the user.

1. What capabilities must users have to ensure proper oversight?

Users must understand the AI system's capacities and limitations, monitor its operation, detect anomalies, address unexpected performance, and be aware of automation bias.

1. How should users interpret the AI system's output?

Users should interpret the output correctly, utilizing available interpretation tools and methods, and have the authority to disregard or override the system's output if necessary.

1. What actions must users be able to take in specific situations?

Users should have the ability to decide not to use the AI system, intervene in its operation, or interrupt it safely, using a "stop" button or similar procedure.

1. What additional requirement applies to certain high-risk AI systems?

For specific high-risk AI systems, the identification resulting from the system must be separately verified and confirmed by at least two competent natural persons before any action or decision is taken based on it.

1. When is the requirement for separate verification not applicable?

The requirement for separate verification does not apply to high-risk AI systems used for law enforcement, migration, border control, or asylum if considered disproportionate under Union or national law.

1. What is the significance of the human-machine interface in oversight?

The human-machine interface is crucial for enabling natural persons to effectively monitor the AI system's operation, understand its output, and intervene when necessary.

1. How does human oversight contribute to risk management in high-risk AI systems?

Human oversight plays a vital role in risk management by ensuring that AI systems are used responsibly, with human intervention available to address potential risks and anomalies as they arise.

1. What role do market surveillance authorities play regarding testing in real world conditions under the AI Regulation?

Market surveillance authorities ensure that testing in real world conditions complies with the requirements outlined in the Regulation.

1. How do market surveillance authorities supervise testing conducted within AI regulatory sandboxes?

They verify compliance with the provisions of the Regulation applicable to AI regulatory sandboxes and may allow derogations from certain conditions if appropriate.

1. What actions can market surveillance authorities take if they suspect non-compliance during testing?

They have the authority to suspend or terminate testing, or require modifications to be made by the provider or prospective provider and user(s).

1. What information must market surveillance authorities provide when issuing a decision or objection regarding testing?

The decision or objection must include the grounds for the action taken and the modalities and conditions for challenging it.

1. How do market surveillance authorities coordinate with other Member States regarding testing decisions?

They communicate the grounds for their decisions to the market surveillance authorities of other Member States where the AI system has been tested, if applicable.

1. What are the requirements for the data used in the development of high-risk AI systems?

High-risk AI systems must be developed using training, validation, and testing data sets that meet specified quality criteria.

1. What data governance and management practices should be applied to training, validation, and testing data sets?

Practices should include considerations such as data collection processes, data preparation operations, bias detection and mitigation measures, and addressing data gaps or shortcomings.

1. What characteristics should training, validation, and testing datasets possess?

They should be relevant, sufficiently representative, error-free, complete, and possess appropriate statistical properties relative to the intended purpose of the AI system.

1. How should datasets account for specific contextual settings where high-risk AI systems are intended to be used?

Datasets should reflect the particular geographical, contextual, behavioral, or functional settings relevant to the intended deployment of the AI system.

1. Under what conditions can providers process special categories of personal data for bias detection and correction?

Processing of special categories of personal data is permitted only if it's strictly necessary, subject to technical limitations and appropriate safeguards, and deleted once the bias is corrected.

1. When are providers allowed to process special categories of personal data for bias detection and correction?

Only when bias detection and correction cannot be effectively achieved through processing other data, and subject to stringent security and privacy measures.

97. What measures must be in place to ensure the security of special categories of personal data processed for bias detection and correction?

Strict controls, documentation of access, confidentiality obligations, and limitations on transmission or access by other parties must be enforced.

98. What happens to the special categories of personal data once bias correction is completed?

The data must be deleted once bias correction is done or when the data reaches the end of its retention period, whichever comes first.

99. What documentation is required regarding the processing of special categories of personal data for bias detection and correction?

Records of processing activities must justify why such processing was necessary and why other data processing methods couldn't achieve the same objective.

100. How do the requirements for data sets differ for high-risk AI systems not using training model techniques?

For such systems, the requirements outlined in paragraphs 2 to 5 apply only to testing data sets.