Draft

ACT

of … 2024

on the digital economy and amending certain related acts

Parliament has adopted the following Act of the Czech Republic:

PART ONE
DIGITAL ECONOMY

Title I
Introductory provisions

§ 1
Subject matter

This Act regulates legal relations related to the dissemination of commercial communications and the performance of the activities of information society service providers and recognised data altruism organisations. This Act incorporates relevant European Union legislation[1)], builds upon directly applicable European Union legislation[2)] and, in the field of the digital economy, regulates

a) competence of public authorities;

b) certain procedural steps applied in the implementation of European Union regulations[1), 2)],

c) the rights and obligations of persons; and

d) liability for infractions of directly applicable European Union legislation[2)] and this Act.

[1)] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[2)] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation).
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation).

§ 2

Definitions

For the purposes of this Act,

a) information society service means a service provided without the simultaneous presence of the parties, by electronic means, at the individual request of a recipient of the service, by means of data transmission and, as a general rule, against payment;

b) electronic mail means a text, voice, audio or video message transmitted via a public communications network that may be stored in the network or on the user's terminal equipment until it is collected by the user;

c) an electronically provided service means a service provided from the point of origin and received at its destination by means of electronic devices for the processing, including digital compression, and storage of data, and wholly transmitted, conveyed, or received by wire, by radio, by optical means, or by other electromagnetic means;

d) a user means a person who uses an information society service;

e) a commercial communication means all forms of communication, including advertising and invitations to visit websites, intended to directly or indirectly promote the goods, services or reputation of an entrepreneur or a person exercising a regulated activity pursuant to § 3(1)(e) of the Act on the Recognition of Professional Qualifications;

f) a Member State of the European Union means a Member State of the European Union or another state party to the Agreement on the European Economic Area;

g) commercial platform means an on-line intermediation service pursuant to Article 2, point (2), of Regulation (EU) 2019/1150 of the European Parliament and of the Council[3)] (hereinafter the ‘Platform-to-Business Regulation’).

Title II

General provisions on information society services

Part 1

Obligation to provide information

§ 3

Information provided to users of the information society service and public authorities

(1) An information society service provider makes the following available in a manner that allows remote access:

[3)] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

a) their contact details, including a contact for the delivery of electronic mail or other means of communication enabling rapid, direct, and effective communication;

b) an indication of the competent supervisory or control authority where the exercise of its activity is subject to an authorisation, consent or concession issued by that authority; and

c) a tax identification number or similar identifier issued by another Member State of the European Union, if the information society service provider is subject to value added tax.

(2) If the information society service provider is a member of a professional chamber with compulsory membership or a person who is a member of a professional chamber having its registered office in another Member State of the European Union and who pursues a regulated activity pursuant to § 3(1)(e) of the Act on the Recognition of Professional Qualifications (hereinafter 'regulated activity'), they shall also make available, in a manner allowing remote access,

a) the name of the professional chamber of which they are a member;

b) professional title pursuant to legislation of a Member State of the European Union governing the pursuit of a regulated activity or the establishment of a professional chamber[4)] and the Member State of the European Union in which the information society service provider has been awarded that professional title; and

c) a reference to the professional rules laid down by this professional chamber.

(3) Information on price provided in connection with the information society service shall be provided in a clear and comprehensible manner so as to make it clear whether the price is inclusive of all taxes, fees and other similar payments.

(4) If a provider of an information society service disseminates a commercial communication that is part of or constitutes an information society service provided by that provider, it must

a) be clearly and conspicuously recognisable as a commercial communication and

b) enable unambiguous identification of the trader in whose name or on whose behalf the commercial communication is disseminated.

Part 2
Country of origin principle

§ 4
Establishment

4

4) For example, Act No 220/1991 on the Czech Medical Chamber, the Czech Dental Chamber and the Czech Chamber of Pharmacists, as amended, Act No 381/1991 on the Chamber of Veterinary Surgeons of the Czech Republic, as amended, Act No 85/1996 on the Legal Profession, as amended, Act No 417/2004 on Patent Attorneys and amending the Act on Measures for the Protection of Industrial Property, as amended.

Establishment for the purposes of this Title means the continuous pursuit of an economic activity through a permanent facility, without this being merely the presence and use of equipment and technology necessary to provide the service.

§ 5

Obligations of an information society service provider established in another Member State of the European Union

(1) The provision of an information society service by a provider established in another Member State of the European Union and providing this service in the Czech Republic may not be restricted under this Act or any other legal regulation of the Czech Republic in the case of legal relationships related to the performance of the activities of information society service providers or access to an information society service.

(2) Notwithstanding paragraph (1), the obligations laid down in this Act or in other legislation of the Czech Republic shall apply to the provision of an information society service by a provider providing that service in the territory of the Czech Republic from its place of establishment in another Member State of the European Union in the following areas:

a) requirements for goods, for the delivery of goods, and for services that are not provided by electronic means;

b) protection of copyright and related rights;

c) protection of the topography of semiconductor products;

d) the protection of the rights of the creator of a database to this database;

e) protection of rights arising from industrial property;

f) the freedom to choose applicable law;

g) consumer protection,

h) requirements to maintain a certain form as a condition for the validity of a legal act establishing, transferring, amending, or cancelling a right in rem in immovable property;

i) the issuance of electronic money by small-scale electronic money issuers;

j) freedom of establishment and freedom to provide services in the field of insurance;

k) compulsory insurance requirements;

l) authorisation of unsolicited commercial communications sent by electronic mail;

m) supervising compliance with the obligations laid down in the Platform-to-Business Regulation and applying liability in the event of breaches thereof.

(3) Paragraph (1) shall apply unless a directly applicable European Union provision provides otherwise.

§ 6

Exceptions to the country of origin principle

(1) A court, law enforcement authority, or public administration body may impose on an information society service provider who provides this service in the Czech Republic from its place of establishment in another Member State of the European Union, notwithstanding § 5(1), an obligation to ensure a legally protected interest in the area of

a) ensuring internal security and public order;

b) the protection of public health,

c) prevention, detection, investigation and prosecution of criminal offences;

d) ensuring the defence of the Czech Republic;

e) consumer protection.

(2) The obligation pursuant to paragraph (1) may be imposed only if the legally protected interests pursuant to paragraph (1) are seriously harmed or threatened by the actions of the information society service provider and if this is necessary and proportionate to safeguard them.

§ 7

Procedure for the application by a public authority of a derogation from the country of origin principle

(1) If a public authority is authorised to impose obligations under § 6, it shall, before imposing the obligation, through the contact point pursuant to § 8(1), ask the Member State of the European Union in which the information society service provider is established to take, within a reasonable period of time, measures to:

a) put an end to the continuing threat or interference with a legally protected interest in the areas pursuant to § 6(1) by the information society service provider;

b) punishing a threat or interference by an information society service provider with a legally protected interest in the areas pursuant to § 6(1); or

c) compensation for damage caused by a threat or interference with a legally protected interest in the areas pursuant to § 6(1).

(2) If the Member State of the European Union in which the provider of the information society service is established fails to take sufficient measures pursuant to paragraph (1) within the prescribed period, these measures shall be taken by the public authority that requested the measure to be taken.

(3) The public authority shall inform the Member State of the European Union in which the information society service provider is established and the European Commission (hereinafter the 'Commission') in advance of its intention to impose an obligation pursuant to § 6 in the manner set out in paragraph (2) through the relevant contact point pursuant to § 8(1); Informing the Member State of the European Union and the Commission is a precondition for taking measures pursuant to paragraph (2).

(4) Where there is a risk of delay, the procedure laid down in paragraphs (1) to (3) shall not apply, and the public authority shall impose the obligation under § 6 itself and inform the Commission and the Member State of the European Union in which the information society service provider is established without undue delay through the relevant contact point pursuant to § 8(1); the information provided must include a justification of the procedure under this paragraph.

§ 8
Contact point

(1) The contact point for cooperation with the Member States of the European Union and the Commission is:

a) the Office for Personal Data Protection in the areas pursuant to § 9 and 10;

b) the Ministry of Industry and Trade in other areas of e-commerce.

(2) The Office for Personal Data Protection shall, without undue delay, ensure the provision of assistance and cooperation to the Member States of the European Union and the Commission in the areas pursuant to § 9 and § 10.

(3) The Ministry of Industry and Trade shall, without undue delay, ensure the provision of assistance and cooperation to the Member States of the European Union and the Commission in other areas of e-commerce.

(4) The contact points shall provide users and providers of information society services the following without undue delay by electronic means:

a) general information on contractual rights and obligations, complaint procedures or the use of remedies in procedures to safeguard and protect rights arising from concluded contracts, including the practical aspects of the use of such procedures;

b) data on persons from whom further information or practical assistance may be obtained in the areas pursuant to subparagraph (a).

Title III
Commercial communications

§ 9
Dissemination of commercial communication

(1) If a business or a person performing a regulated activity has obtained from their customer's email address in connection with the sale of a product or service, they may use it for the dissemination of commercial communication concerning another similar product or service offered by them by electronic means only provided that:

a) the customer, when providing their email address, did not refuse such use, although the entrepreneur or a person performing a regulated activity allowed them to do so free of charge, in a simple and comprehensible manner;

b) the customer may at any time, free of charge and in a simple and comprehensible manner, refuse the use of their email address, even in the case of each individual message being sent; and

c) no more than 2 years have elapsed since the last commercial communication was sent to the customer.

(2) Where a trader or a person exercising a regulated activity has not obtained an email address in connection with the sale of a product or service, that address may be used for the dissemination of commercial communications by electronic means only in relation to users who have given their prior consent within the meaning of Article 4(11) of Regulation (EU) 2016/679 of the European Parliament and of the Council.[5)].

(3) The sending of electronic mail for the purpose of distributing a commercial communication is prohibited if this commercial communication

a) is not clearly and unambiguously identified as a commercial communication;

b) does not make it possible to identify unambiguously and to the extent necessary the entrepreneur or the person performing the regulated activity in whose name or on whose behalf the communication takes place; or

c) is sent without information that the user or customer can directly and effectively refuse the use of their email address or to withdraw their consent to the sending of commercial communications.

§ 10
Commercial communications by members of professional chambers

(1) A member of a professional chamber with compulsory membership or a person who is a member of a professional chamber established in another Member State of the European Union and who pursues a regulated activity may, using electronic means in the context of activities which are the content of a regulated profession, disseminate commercial communications under the conditions laid down in § 9 and in accordance with the professional rules issued by those professional chambers, which govern, in particular, the rules of independence, honesty, professionalism, dignity and reputation of the profession or status, the protection of business or other professional secrets, or

[5)] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

the rules of fair treatment of customers and other participants in the pursuit of a regulated profession.

(2) Commercial communication from a member of a professional association with compulsory membership or from a member of a professional association established in another Member State of the European Union carrying out a regulated activity contains

a) the name of the professional chamber of which the person disseminating the commercial communication is a member;

b) reference to the professional rules applied by this professional chamber; and

c) a reference to information about this professional chamber available in a manner allowing remote access.

§ 11
Judicial protection

A provider of an information society service whose commercial interests are harmed by a breach of the obligations under § 9 or 10 shall have the same rights as in the protection against unfair competition.

Title IV
Some procedures related to the Digital Services Regulation

§ 12
Issuing orders to remove content and to provide information

If a public authority issues an order on the basis of other legislation[6)] pursuant to Article 9 or 10 of Regulation (EU) 2022/2065 of the European Parliament and of the Council[7)] (hereinafter the 'Digital Services Regulation'), it shall indicate this in the order being issued.

§ 13
General provision for certain procedures under the Digital Services Regulation

(1) An application for certification as an out-of-court dispute resolution body, trusted flagger status, and vetted researcher status can also be submitted on the form pursuant the Act on the Right to Digital Services[8)], which the Czech Telecommunication Office (hereinafter the 'Office') shall make available in a manner allowing remote access.

[6)] For example, § 8e of Act No 141/1961 on judicial criminal proceedings (the Criminal Code), as amended
[7)] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation).
[8)] Act No 12/2020 on the right to digital services and amending certain acts, as amended.

(2) Documents demonstrating compliance with the condition for granting certification as an out-of-court dispute settlement body pursuant to Article 21(3) of the Digital Services Regulation, the condition for granting the status of trusted flagger pursuant to Article 22(2) of this Regulation, or the condition for granting the status of vetted researcher pursuant to Article 40(8) of this Regulation may be replaced by a declaration on honour where there are significant objective obstacles to their procurement or where their procurement would involve disproportionate effort or costs; the impossibility of obtaining the required documents must be demonstrated by the applicant in such cases.

§ 14
Obligation to provide information

(1) If there are changes in the facts relating to the conditions for granting certification of an out-of-court dispute resolution body pursuant to Article 21(3) of the Digital Services Regulation, trusted flagger status pursuant to Article 22(2) of this Regulation or the conditions for granting the status of a vetted researcher pursuant to Article 40(8) of this Regulation, the holder of the status or certification shall notify the Office of any such changes within 15 days of the date on which they occurred.

(2) The notification pursuant to paragraph (1) may be submitted using the form provided for in the Act on the Right to Digital Services[8)], which the Office shall make available in a manner allowing remote access.

§ 15
Certification of an out-of-court dispute resolution body

(1) Decision on the certification of the out-of-court dispute settlement body and decision on the extension period of its validity shall be considered as a certificate pursuant to the second subparagraph of Article 21(3) of the Digital Services Regulation.

(2) Certification of the out-of-court dispute resolution body shall cease as set out in Article 21(7) of the Digital Services Regulation or on the date on which notification of the body for out-of-court dispute settlement of the cessation of its activities was delivered to the Office, unless such notification indicates the date of cessation of activities as a later date.

§ 16
Suspension of activities and termination of the status of trusted flagger

(1) The Office shall suspend the activities of a trusted flagger by means of an interim measure where it has initiated proceedings to withdraw the status of trusted flagger pursuant to Article 22(7) of the Digital Services Regulation.

(2) The status of trusted flagger shall cease in the manner set out in Article 22(7) of the Digital Services Regulation or on the date on which the notice of cessation of the activities of the trusted flagger is received by the Office, unless the notice indicates a later date of cessation.

§ 17

Cross-border referral of an application for the status of approved researcher

(1) If the application for the status of vetted researcher pursuant to Article 40(9) of the Digital Services Regulation does not contain the required elements or suffers from other defects that prevent the initial full assessment of the application, the Office shall invite the applicant to remedy the deficiencies of the application and give him or her a reasonable period of time to do so. If the applicant fails to remedy the deficiencies or defects identified within the set time limit, the Office shall carry out an initial assessment of the application to the extent that the application submitted allows and forward the application to the Digital Services Coordinator in the country of establishment of the provider of the very large online platform or very large online search engine with that partial initial assessment; If the defects in the application rule out the designation of the competent coordinator in the country of establishment, the Office shall only inform the applicant of this fact and send back the paper documents and material data carriers received.

(2) The applicant shall be obliged to provide the Office with all assistance necessary for the initial assessment of its application and for sending it to the Digital Services Coordinator in the country of establishment, and to comply with the Office's requests for its provision.

(3) Where the Office carries out an initial assessment of the application and sends it to the Digital Services Coordinator in the country of establishment pursuant to Article 40(9) of the Digital Services Regulation, it shall notify the applicant thereof and send the applicant the initial assessment of the application for information.

§ 18

Procedures for access to data of the provider of the very large online platform and the very large online search engine

(1) Only the applicant for the status of vetted researcher shall be a party to the application procedure under Article 40(8) of the Digital Services Regulation.

(2) If a decision on a request pursuant to Article 40(8) of the Digital Services Regulation cannot be issued without delay, the Office shall issue it no later than 90 days from the date of the opening of the proceedings.

(3) By means of a measure of a general nature, the Office for Personal Data Protection shall adjust the minimum technical and organisational measures necessary to meet the conditions for the protection of personal data pursuant to Article 40(8)(d) of the Digital Services Regulation.

(4) After being granted the status of vetted researcher, the Office will send a reasoned request for access to data pursuant to Article 40(4) of the Digital Services Regulation

a) the provider of the very large online platform or the very large online search engine indicated in the application for the status of vetted researcher to provide the data specified in the application; and

b) a vetted researcher who is an applicant for access to data.

(5) If the Office fully complies with any of the proposals submitted pursuant to Article 40(6), first subparagraph, of the Digital Services Regulation, it shall notify the provider of the very large online platform or the very large online search engine concerned by sending a new request, which it shall also send to the vetted researcher requesting the disclosure of the data.

(6) If the conditions under paragraph (5) are not met, the Office shall reject or partially reject the request of the provider of the very large online platform or the very large online search engine pursuant to Article 40(5) of the Digital Services Regulation by a decision imposing an obligation on the provider of the very large online platform or the very large online search engine to allow the vetted researcher access to the data included in the decision and specifying the manner and time limit for their provision. Such a decision may be the first act of the Office in the proceedings. An appeal against a decision shall not have suspensory effect. Only the provider of the very large online platform or the very large online search engine concerned shall be a party to the proceedings. The Office shall inform the vetted researcher, who is the applicant for access to the data, of the issuance of the decision and its content in an appropriate manner.

(7) The right of access granted in the context of granting the status of vetted researcher shall lapse in the manner provided for in the Digital Services Regulation or on the date of receipt of the notification by the vetted researcher of the termination of his or her research to the Office, unless such notification indicates a later date for the completion of the research. The Office shall notify the provider of the very large online platform or the very large online search engine concerned of the forfeiture of the right of access by the vetted researcher.

Title V
Some procedures related to the Data Governance Regulation

Part 1
Providers of data intermediation services

§ 19
Confirmation related to providers of data intermediation services

Notification pursuant to Article 11(1) of Regulation (EU) 2022/868 of the European Parliament and of the Council[9)] ('Data Governance Regulation') and an application for a certificate pursuant to Article 11(8) or (9) of this Regulation may also be submitted using the form provided for in the Right to Digital Services Regulation[8)], which the Office shall make available in a manner allowing remote access.

Part 2
Recognised data altruism organisations

§ 20
Register of recognised data altruism organisations

[9)] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation).

The following information regarding a corporate entity shall be entered in the register of recognised data altruism organisations pursuant to Article 19 of the Data Governance Regulation:

a) name;

b) entity identification number or, where applicable, another unique identifier of the corporate entity recorded in the public administration information system;

c) the address of the registered office and the address of the place of business in a Member State of the European Union;

d) the public website of the corporate entity pursuant to Article 19(4)(f) of the Data Governance Regulation;

e) the name of the contact person and that person's email address, if different from the email address pursuant to point (f);

f) phone number and email address of the corporate entity;

g) information on the objectives of general interest that the corporate entity intends to promote in the collection of data;

h) information on the nature of the data that the corporate entity intends to check or process and the categories of personal data in the case of processing personal data;

i) the identity of the representative pursuant to Article 19(3) of the Data Governance Regulation, which are

   1. name, address for delivery in the Czech Republic, and date of birth, in the case of a natural person; or

   2. the name, registered office, and entity identification number, or another unique identifier of the corporate entity recorded in the public administration information system in the case of a corporate entity.

§ 21

Registration of recognised data altruism organisations

(1) An application for registration in the Register of Recognised Data Altruism Organisations pursuant to Article 19(1), (2) or (3) of the Data Governance Regulation may also be submitted using the form provided for in the Right to Digital Services Regulation[8)], which the Office shall make available in a manner allowing remote access.

(2) In the application procedure, a written decision shall be made only if the Office rejects the application; otherwise, it shall proceed in accordance with Article 19(5) of the Data Governance Regulation. The Office shall notify the applicant of the registration pursuant to Article 19(5) of the Data Governance Regulation in writing, without orally announcing the decision.

§ 22

Deletion from the register of recognised data altruism organisations

(1) The Office shall delete a recognised data altruism organisation from the register of recognised data altruism organisations in the manner set out in Article 24(5) of the Data Governance Regulation or on the date of receipt of a notification by a recognised data altruism organisation of the cessation of its activities to the Office, unless such notification indicates a later date for cessation.

(2) The Office shall publish the decision to remove a recognised data altruism organisation from the register of recognised data altruism organisations in a manner allowing remote access.

Title VI

Government administration in the area of the digital economy

Part 1

Competent authorities under directly applicable European Union legislation

§ 23

Competent authorities under the Digital Services Regulation

(1) The competent authorities pursuant to Article 49(1) of the Digital Services Regulation are the Office and the Office for Personal Data Protection.

(2) The Digital Services Coordinator pursuant to Article 49(2) of the Digital Services Regulation is the Office.

(3) The Office shall be competent for proceedings pursuant to §§ 13 to 18.

§ 24

Competent authorities pursuant to the Data Governance Regulation

(1) The Office shall be the competent authority for data intermediation services pursuant to Article 13 of the Data Governance Regulation.

(2) The competent authority for the registration of recognised data altruism organisations pursuant to Article 23 of the Data Governance Regulation is the Office.

Part 2

Supervisory authorities and their cooperation +

§ 25

Supervisory authorities for compliance with obligations in the field of commercial communications

The authority competent to supervise compliance with the obligations under Title III is

a) the Office for Personal Data Protection for compliance with the conditions for the dissemination of commercial communications laid down in § 9;

b) the competent professional chamber with compulsory membership for the obligations laid down in § 10, in the case of its members.

§ 26

Supervisory authority for compliance with the Platform-to-Business Regulation

The authority competent to supervise compliance with the obligations laid down in the Platform-to-Business Regulation is the Office.

§ 27

Supervisory authorities for compliance with the Digital Services Regulation

(1) The Office shall be competent to supervise compliance with the obligations under the Digital Services Regulation, unless otherwise provided for in this Act.

(2) The Office for Personal Data Protection is the competent authority to supervise compliance with the obligations set out in Articles 26 and 28(2) of the Digital Services Regulation.

§ 28

Supervisory authority for compliance with the Data Governance Regulation

The Office is the authority competent to supervise compliance with the obligations of providers of data intermediation services and recognised data altruism organisations established by the Data Governance Regulation.

§ 29

Cooperation between supervisory authorities

(1) The Office and the Office for Personal Data Protection provide each other with information that may contribute to the proper performance of supervision under this Act, including information of a confidential nature. For the information provided, the recipient must ensure the same level of confidentiality as that established by the providing authority.

(2) A public authority exercising supervision in a field of public administration other than authorities pursuant to paragraph (1) shall provide the Office or the Office for Personal Data Protection, at their request and without undue delay, information obtained in the exercise of its competence that may contribute to the proper exercise of supervision under this Act, including information of a confidential nature. For the information provided, the recipient must ensure the same level of confidentiality as that established by the providing authority.

(3) If an inspection carried out by the Office for Personal Data Protection relates to compliance with the requirements pursuant to Article 40(8)(d) of the Digital Services Regulation by a vetted researcher, the Office for Personal Data Protection shall send a copy of the inspection report and a copy of the settlement of objections to the inspection finding, if objections have been submitted, to the Office after the inspection has been completed.

(4) If the Office submits an application to the Office for Personal Data Protection to carry out an inspection related to the fulfilment of the requirements arising from Article 40(8)(d) DSA by a vetted researcher, the Office for Personal Data Protection shall, without undue delay after its settlement, inform the Office of the manner and conclusions of the handling of the application.

(5) If the proceedings conducted by the Office under this Act are related to compliance with an obligation under the legal regulations governing the processing and protection of personal data, the Office may request the opinion of the Office for Personal Data Protection.

§ 30

Cooperation in the preparation of an activity report pursuant to the Digital Services Regulation

(1) A public authority that is not a Digital Services Coordinator pursuant to this Act and that issued an order pursuant to Article 9 or 10 of the Digital Services Regulation in the relevant calendar year shall provide the Office with all information necessary for the preparation of the activity report pursuant to Article 55 of the Digital Services Regulation, at the latest by the end of February of the calendar year following the calendar year for which the Office prepares the activity report.

(2) A public authority that participates in the exercise of supervision under the Digital Services Regulation pursuant to this Act shall, upon request, provide the Office with the information necessary for the processing of the activity report pursuant to paragraph (1); In the request, the Office shall specify the time limit, the scope, and the manner in which the requested information is to be provided.

(3) If orders pursuant to Article 9 or 10 of the Digital Services Regulation have been issued in criminal proceedings, the competent authority shall, within the period pursuant to paragraph (1), provide the Office only with summary information on the number of such orders issued in the relevant calendar year and on the nature of the information covered by the orders. If the provision of summary information on the nature of the information to which the orders related would jeopardise the achievement of the purpose of the proceedings in the case concerned or in a related case, the information shall not be provided. Information on pre-trial orders issued by public prosecutors shall be provided to the Office collectively on behalf of the Public Prosecutor’s Office by the Supreme Public Prosecutor’s Office, and information on other pre-trial orders shall be provided collectively on behalf of the police authorities of the Police of the Czech Republic; the police and the public prosecutor's office shall send the necessary information to these aggregated data processors no later than the end of January of the calendar year for the previous calendar year. Information on orders issued in court proceedings shall be provided to the Office by the individual courts.

§ 31

Cooperation pursuant to the Digital Services Regulation

(1) The actions of the Digital Services Coordinator of another Member State of the European Union, which has been requested by the Office to provide assistance pursuant to Article 57(2) and (3) or Article 60(4) of the Digital Services Regulation, may be used as part of the pre-inspection actions to assess whether to initiate an inspection or as supporting documents for the Office's inspection findings in the context of an initiated inspection.

(2) If the Office requests the Digital Services Coordinator of another Member State of the European Union to cooperate in the service of a document abroad, it may also be served in electronic form in the manner laid down by the law of the Member State of the European Union of that coordinator for the service of similar documents.

(3) An employee of the Office has the rights and obligations of an inspector under the Inspection Code and this Act in actions pursuant to Article 57(2) and (3) or Article 60(4) of the Digital Services Regulation, with the exception of the obligation to draw up an inspection report; they shall forward their findings, including the evidence gathered, to the Digital Services Coordinator of another Member State of the European Union that requested the Authority to provide assistance pursuant to Article 57(2) and (3) or Article 60(4) of the Digital Services Regulation.

(4) Paragraph (3) shall apply mutatis mutandis to the provision of assistance to the Commission under the Digital Services Regulation.

§ 32

Cooperation in ensuring participation in the activities of the European Board for Digital Services

If the Office or the Office for Personal Data Protection finds that a matter dealt with by the European Board for Digital Services affects the competence of the Office for Personal Data Protection, a representative of this authority shall also attend the meetings of the Board pursuant to Article 62 of the Digital Services Regulation. Where the deliberations of the European Board for Digital Services are not convened in a case related to Article 26 or 28(2) of the Digital Services Regulation, the Office for Personal Data Protection may merely provide the Office with an opinion on the pending case, which the representative of the Office shall take into account when voting in that Board.

§ 33

Synergies pursuant to the Data Governance Regulation

The Office shall have the same powers of cooperation pursuant to Article 14(7), Article 24(6), and Article 26(6) of the Data Governance Regulation as in the exercise of the oversight for which it is competent pursuant to Article 11(2) or Article 19(2) of this Regulation.

Part 3

Common provisions on the conditions for the exercise of supervision of compliance with directly applicable regulations pursuant to this Act

§ 34

Obligation of confidentiality

(1) An official involved in the supervision of compliance with the P2B Regulation, the Digital Services Regulation, or the Data Governance Regulation, unless it concerns the re-use of data held by public sector bodies, or in cooperation pursuant to § 29, shall maintain confidentiality of all facts of which he or she has become aware in connection with the performance of such supervision or in connection with the performance of the activities by which the requested cooperation is ensured in the context of the supervision carried out.

(2) The duty of confidentiality of a public official continues even after the termination of their service, employment or similar legal relationship.

(3) The official may be released from the obligation of confidentiality by the person in whose interest the official has this obligation, or in the public interest by the head of the administrative body in relation to whose competence in the field of supervision or cooperation the obligation of confidentiality has arisen.

(4) The obligation of confidentiality shall apply mutatis mutandis to other natural persons involved in the exercise of supervision in the areas pursuant to paragraph (1).

§ 35

Obligation to provide information

(1) A person set out in Article 51(1)(a) of the Digital Services Regulation, a provider of a trading platform, a provider of an online search engine, a provider of data intermediation services, or a recognised data altruism organisation shall provide a supervisory authority pursuant to this Act, upon its request, with complete and truthful information, including financial and other information, that is necessary to carry out the activities for which the supervisory authority is competent under this Act. In the letter of formal notice, the supervisory authority shall specify a reasonable period, the scope, and the manner in which the information is to be provided. The request from the supervisory authority shall include a statement of reasons, indicating the purpose for which the information is required by the supervisory authority. The supervisory authority may only request information that is proportionate to the purpose for which it is obtained.

(2) The information provided by the person pursuant paragraph (1) to the supervisory authority must be protected by this authority against misuse, damage, destruction, unauthorised alteration, loss or theft.

(3) Paragraph (1) is without prejudice to the obligation of the person involved in the supervision to prove authorisation to access classified information.

§ 36

Special provisions on inspection

(1) The authorisation to carry out inspections under this Title also takes the form of an identification card, the specimen of which shall be laid down in a decree of the Ministry of Industry and Trade.

(2) If the subject-matter of the inspection so requires and if the purpose of the inspection cannot be achieved otherwise, civil servants assigned to the Office and employees working in the Office in a basic employment relationship authorised to perform the Office's inspection tasks pursuant to this Act shall be entitled, in exceptional cases and to the extent necessary, to act under a changed identity, including the use of a cover document or related data kept in the public administration information system.

(3) The use of a cover document or related data held in the public administration information system for the purposes of an individual inspection requires the prior consent of the Chairman of the Board of the Office.

(4) Inspection under this Title also commences with the first act of acting under a changed identity or using a cover document in order to obtain the information necessary for the exercise of inspection under this Title. In the procedure pursuant to the first sentence, the inspector shall inform the inspected person of the commencement of the inspection at a time when it does not jeopardise the fulfilment of the purpose or the performance of the inspection.

(5) When checking compliance with the Digital Services Regulation, the inspector of the Office or the Office for Personal Data Protection may, with the prior consent of the court, enter a dwelling that is not used for business or other economic activities, if there are reasonable grounds to suspect that business books or other records that may be relevant to achieving the purpose of the inspection are present in the dwelling, and the dwelling is owned or used by

a) an entity set out in point (a) of Article 51(1) or Article 67(1) of the Digital Services Regulation;

b) a member of the statutory body of an entity set out in point (a); or

c) a person in an employment or similar relationship with an entity set out in subparagraph (a).

§ 37
Acts of a person under a changed identity

(1) If an inspector acts under a changed identity when performing inspection as a person who expresses the will to enter into a contract with the inspected person, the conduct of the inspector shall be regarded as his or her legal act.

(2) The inspector may withdraw from the contract concluded pursuant to paragraph (1) if it is demonstrated that the contract was concluded during the inspection and if this does not cause financial harm to the inspected party.

§ 38
Cover documents

(1) Cover document means a document or other instrument used to conceal the true identity of a natural person and to prevent disclosure of the Office's inspection activities.

(2) The issuance of a cover document is decided by the Minister of Industry and Trade on a proposal from the Chairman of the Board of the Office. The Ministry of the Interior shall issue or obtain a cover document at the request of the Office.

(3) A cover document may not be an ID card of a deputy or senator, a member of the government, a member of the Bank Board of the Czech National Bank, a member of the college of the Supreme Audit Office, a judge of the Constitutional Court, a service ID card of a judge or a public prosecutor, a service ID card of a security corps employee, a service ID card of a member of the security corps, a service ID card of a member of the intelligence service of the Czech Republic, a military document pursuant to the Armed Forces Act, or a document of a living or deceased person.

(4) If it is necessary due to the nature of the cover document, the Ministry of the Interior is entitled, when procuring or issuing the cover document, to ensure, to the extent necessary, in public administration information systems maintained under other legislation[10)] the entry, modification, blocking, or destruction of data related to the issue and use of the cover document. The administrator of the public administration information system shall provide the necessary cooperation to carry out information activities to the specified extent and to ensure their purpose, while proceeding in such a way that the activities of the Ministry of the Interior or the Office are not disclosed.

(5) Records of cover documents issued or provided by the Ministry of the Interior are kept simultaneously by the Ministry of the Interior and the Office.

(6) At the request of the Office, the Ministry of the Interior shall implement measures for the data protection of cover documents.

(7) The Office protects cover documents from misuse.

Part 4
Supervision of compliance with the Digital Services Regulation

§ 39
Action Plan

(1) Where the conditions laid down in the first subparagraph of Article 51(3) of the Digital Services Regulation are met, the Office or the Data Protection Authority shall, ex officio or following a request from the Commission pursuant to Article 82(1) of the Digital Services Regulation, invite providers of intermediary services to draw up an action plan pursuant to point (a) of the first subparagraph of Article 51(3) of the Digital Services Regulation and set a reasonable deadline for its submission.

(2) The action plan pursuant to paragraph (1) shall contain, in particular:

a) a list of the measures necessary to bring the infringement to an end and a detailed statement of the reasons for the proposed measures;

[10)] Act No 365/2000 on public service information systems and amending certain other acts, as amended.

b) the time limits for the implementation of the measures referred to in point (a) and the reasons therefor;

c) the deadline for submitting the report on the manner of implementing the measures pursuant to point (a) and the period during which the measures will be implemented;

d) the deadline for submitting the report on the evaluation of the measures taken.

(3) The Office or the Office for Personal Data Protection shall assess the action plan submitted by the provider of intermediary services and inform the provider of intermediary services, which is its processor, in writing within 2 months of the date of submission of the action plan that

a) it agrees with the proposed measures; or

b) the submitted action plan is deemed insufficient to terminate the infringement and provides the reasons for this inadequacy; where appropriate, it shall invite providers of intermediary services to supplement or otherwise modify this action plan.

§ 40

Comments on the proposal for a temporary restriction on access to a service

The provider of an intermediary service to which access is to be restricted under the envisaged measure shall be invited to submit comments pursuant to the second subparagraph of Article 51(3) of the Digital Services Regulation via the contact point pursuant to Article 11 of the Digital Services Regulation; the invitation shall be deemed to have been received on the expiry of the tenth day following its dispatch. Other stakeholders and the provider of an intermediary service to which access is to be restricted under the envisaged measure for failing to comply with the obligation under Article 11 of the Digital Services Regulation are invited to submit comments pursuant to the first sentence by publishing a notice on the electronic bulletin board of the authority concerned.

§ 41

List of services with temporarily restricted access

(1) The Office shall maintain and publish on its website, in a machine-readable format, a list of services with temporarily restricted access, in which it shall enter the website to which the provider of the internet access service is to refuse access pursuant to a court order under point (b) of the first subparagraph of Article 51(3) of the Digital Services Regulation.

(2) The entry in the list pursuant to paragraph (1), its amendment or deletion shall be effected by the Office without delay upon receipt of a court decision pursuant to point (b) of the first subparagraph of Article 51(3) of the Digital Services Regulation, upon receipt of a decision of the Office for Personal Data Protection, the issuance of its own decision pursuant to § 42(3), or upon receipt of a decision amending or repealing any of those decisions, or if it finds, of its own motion or on the basis of an initiative, that the entry does not correspond to the decision issued.

(3) The list pursuant to paragraph (1) shall contain the address of the website, the date of publication of its inclusion in the list, and the date on which the period of access restriction pursuant to the third subparagraph of Article 51(3) of the Digital Services Regulation expires, starting from

the date of publication of the inclusion of the website in that list. If the period pursuant to the first sentence has been extended by a decision of the Office or the Office for Personal Data Protection pursuant to § 42(3), the Office shall without delay amend the record of the date of expiry of the period of restriction of access in accordance with this decision.

(4) The provider of an internet access service in the Czech Republic shall be obliged to prevent access to a website included in the list pursuant to paragraph (1) at the latest from the fifth day following the date of publication of such registration until the date of expiry of the period of restriction of access specified in the list pursuant to paragraph (1).

§ 42

Proceedings to extend the period of restricted access to a service

(1) Party to the proceedings to extend the access restriction period pursuant to the third subparagraph of Article 51(3) of the Digital Services Regulation is only the one who was the party to the preceding proceeding in the case, with the exception of the Office or the Office for Personal Data Protection as the petitioner.

(2) In the proceedings pursuant to paragraph (1), documents shall be served by public notice, with the exception of documents sent to the addressee of a court decision pursuant to point (b) of the first subparagraph of Article 51(3) of the Digital Services Regulation who is effectively involved in ensuring the temporary restriction of access to a service other than as an internet access service provider, and to the provider of an intermediary service in relation to which the period of access restriction is to be extended, if they have fulfilled their obligation under Article 11 of the Digital Services Regulation or have an accessible data mailbox, to which documents are served in the manner laid down in the first sentence of § 40 or to a data mailbox.

(3) The decision to extend the period of access restriction pursuant to the third subparagraph of Article 51(3) of the Digital Services Regulation shall be issued by the Office or the Office for Personal Data Protection as the first step in the proceedings. An appeal against the decision pursuant to the first sentence has no suspensory effect; the decision must be issued before the access restriction period expires.

(4) If the Office for Personal Data Protection issues a decision pursuant to paragraph (3), it shall send a copy thereof to the Office.

§ 43

Corrective measures

If the Office or the Office for Personal Data Protection finds that a enterpreneur has breached any of the obligations under § 9 or that a provider of intermediary services has breached the Digital Services Regulation, it may impose corrective measures on the entrepreneur or provider of intermediary services consisting of

a) laying down specific conditions for the provision of an intermediation service or the dissemination of commercial communications;

b) refraining from any action related to the provision of an intermediation service or the dissemination of commercial communications; or

c) imposing an additional obligation not set out in points (a) and (b) related to the provision of an intermediary service or the dissemination of commercial communications.

§ 44
Concurrent proceedings

If the Office or the Office for Personal Data Protection has initiated proceedings concerning an infringement of the Digital Services Regulation and the Commission initiates proceedings under the Digital Services Regulation on the same matter, the Office or the Office for Personal Data Protection shall discontinue the proceedings it has initiated.

Section 5
Supervision of compliance with the Data Governance Regulation

§ 45
Postponement of the commencement or suspension of the provision of data intermediation services

The Office shall issue a decision to defer the commencement or suspend the provision of data intermediation services under the Data Governance Regulation as the first step in the proceedings. An appeal against this decision shall not have suspensory effect.

Title VII
Liability for breaches of obligations

Section 1
Special procedures related to breaches of obligations

§ 46
Infringement notice

(1) If the Office or the Office for Personal Data Protection considers that a person who is subject to an obligation imposed by the Platform-to-Business Regulation, the Digital Services Regulation, the Data Governance Regulation or this Act, the breach of which is established as an infraction under this Act, has breached this obligation in a less serious manner, it may, instead of initiating infraction proceedings, bring the infringement to the attention of the infringer.

(2) In the notice pursuant to paragraph (1), the Office or the Office for Personal Data Protection shall state what it sees as a breach of obligations and shall call on the infringer to terminate the unlawful activity or to remedy the consequences of unjustified interference with the rights and legally protected interests of third parties; at the same time, the Office or the Office for Personal

Data Protection shall set in the notice a deadline for the termination of the unlawful activity, or for the remedy of unjustified interference with the rights and legally protected interests of third parties. If Article 14(3) or Article 24(3) of the Data Governance Regulation does not apply, the deadline pursuant to the first sentence shall not be less than 15 days from the date of receipt of the notification.

(3) If a person has received a notice from the Office or the Office for Personal Data Protection pursuant to paragraph (1), they shall remedy the unlawful situation by the deadline set out in the notice and subsequently notify the supervisory authority that alerted them to the breach of obligations of this without delay; in the notification, this person shall at the same time list the measures they have taken to put an end to the unlawful situation.

(4) If the Office or the Office for Personal Data Protection assesses the notification pursuant to paragraph (3), in particular the measures referred to therein, as insufficient or, on its own initiative or on the basis of a third party's notification, assesses the remedy as insufficient, it shall initiate infraction proceedings in the matter. The Office or the Office for Personal Data Protection shall also initiate proceedings on an infraction in the matter in question if the infringer fails to deliver the notification pursuant to paragraph (3) within 15 days of the expiry of the period for remedying the unlawful situation set for the infringer in the notification pursuant to paragraph (2).

(5) If the Office or the Office for Personal Data Protection assesses the notification pursuant to paragraph (3) as sufficient, it shall not initiate infraction proceedings and shall close the case by a resolution. The decision to close the case shall be noted in the case file.

§ 47

Acceptance of commitments by providers of intermediary services

(1) If the Office or the Office for Personal Data Protection conducts infraction proceedings pursuant to §§ 50 to 56, the provider of intermediary services may propose to the Office or the Office for Personal Data Protection commitments providing guarantees to ensure continued compliance with the Digital Services Regulation and this Act.

(2) The provider of intermediary services may propose commitments pursuant to paragraph (1) to the Office or the Office for Personal Data Protection in writing no later than by the end of the period for commenting on the documents supporting the decision.

(3) The provider of intermediary services shall be bound by its draft commitments to the Office, the Office for Personal Data Protection, or to third parties from the date on which the decision on the conditional waiver of the imposition of an administrative penalty pursuant to paragraph (4) becomes final.

(4) The Office or the Office for Personal Data Protection shall conditionally refrain from imposing an administrative penalty if the proposed commitments are sufficient to achieve their purpose pursuant to paragraph (1) and, given the nature and seriousness of the infraction committed and the person of the offender, it can be reasonably expected that the handling of the case by the Office or the Office for Personal Data Protection alone will suffice to remedy it. If material damage has been caused by the offender’s conduct, § 42(2) of the Act on liability for and proceedings on infractions shall apply mutatis mutandis.

(5) If the conditions for a conditional waiver of the imposition of an administrative penalty pursuant to paragraph (4) are not met, the Office or the Office for Personal Data Protection shall find the proposed commitments insufficient to achieve their stated purpose and shall justify this fact in the decision on the infraction.

(6) The Office or the Office for Personal Data Protection may, by a new decision, revoke the decision on the conditional waiver of the imposition of an administrative penalty pursuant to paragraph (4) and impose an administrative penalty on the offender if

a) the provider of intermediary services acted in breach of the proposed commitments;

b) the assessment of the proposed commitments pursuant to paragraph (1) was carried out by the Office or the Office for Personal Data Protection on the basis of incomplete, incorrect, or misleading information provided by the provider of intermediary services; or

c) the condition pursuant to § 99(2) of the Act on liability for and proceedings on infractions has been met.

Section 2
Infractions

§ 48
Infractions related to the dissemination of commercial communications

(1) A natural person commits an infraction by disseminating commercial communications in bulk or repeatedly by electronic means without the consent of the addressee.

(2) Legal entities or sole traders commit an infraction by disseminating commercial communications in bulk or repeatedly by electronic means

a) without lawful reason;

b) without giving the customer, when concluding a contract for the sale of a product or service, the opportunity to refuse, in a clear, distinct, simple manner and free of charge, the use of their email address for such dissemination of commercial communications;

c) without giving the customer with the opportunity to refuse, in a clear, distinct, simple manner and free of charge, the use of their email address with each individual message; or

d) after 2 years have passed from the date the last commercial communication was sent to the customer.

(3) Legal entities or sole traders commit an infraction by disseminating commercial communications in bulk or repeatedly via email

a) that are not clearly and unambiguously marked as commercial communications;

b) that do not make it possible to identify unambiguously and to the extent necessary the entrepreneur or the person performing the regulated activity in whose name or on whose behalf the communication takes place; or

c) without information on the possibility for the user to directly and effectively deliver a refusal to use their email address or to withdraw their consent to the sending of commercial communications.

(4) Legal entities or sole traders who are members of a professional association with compulsory membership or members of a professional association established in another Member State of the European Union carrying out a regulated activity shall commit an infraction if their commercial communication does not contain

a) the name of the professional chamber of which the person disseminating the commercial communication is a member;

b) a reference to the professional rules applied by that professional chamber; or

c) a reference to information about this professional chamber available in a manner allowing remote access.

(5) For an infraction, a fine may be imposed up to the amount of

a) CZK 100,000 in the case of an infraction pursuant to paragraph (1);

b) CZK 1,000,000 in the case of an infraction pursuant to paragraph (4); or

c) an amount equivalent to EUR 20,000,000 or, where the offender is an undertaking pursuant to point (18) of Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council[5)], up to 4% of the offender's net worldwide turnover in the last completed financial year, whichever is higher, in the case of infractions pursuant to paragraphs (2) and (3).

§ 49

Infractions committed by providers of e-commerce platforms and online search engines

(1) An e-commerce platform provider commits an offence by

a) failing to ensure that its conditions meet the requirements pursuant to Article 3(1) of the Platform-to-Business Regulation;

b) failing, contrary to Article 3(2) of the Platform-Business Relations Regulation, to notify business users of changes to their terms and conditions on a durable medium or implementing proposed changes before the deadline for their notification;

c) failing to ensure clear visibility of the identity of the business user providing goods and services through an e-commerce platform pursuant to Article 3(5) of the Platform-Business Relations Regulation;

d) restricting, suspending or terminating the provision of an e-commerce platform contrary to Article 4 of the Platform-Business Relations Regulation;

e) failing to set out in its terms and conditions the main parameters and the reasons for the relative importance of those main parameters pursuant to Article 5(1), (3) and (5) of the Platform-Business Relations Regulation;

f) failing, contrary to Article 6 of the Platform-Business Relationship Regulation, to provide in its terms and conditions a description of the type of ancillary goods and services offered, including financial products, or a description of whether and under which circumstances a business user may offer its own ancillary goods and services through an e-commerce platform;

g) failing, contrary to Article 7(1) of the Platform-to-Business Regulation, to describe in its terms and conditions the differentiated treatment it applies or may apply in relation to goods and services offered to consumers through the e-commerce platform either by that provider itself or by business users under its control or by other business users;

h) failing to ensure that the terms and conditions comply with Article 8 of the Platform-to-Business Regulation;

i) failing, contrary to Article 9(1) of the Platform-to-Business Regulation, to describe in its terms and conditions the technical and contractual access of business users to personal data or other data that business users or consumers provide for the use of the e-commerce platform or that are generated in the provision of that service, or failing to indicate that there is no technical and contractual access;

j) failing to comply with the information obligation pursuant to Article 9(2) of the Platform to Business Regulation;

k) failing, contrary to Article 10 of the Platform-to-Business Regulation, to state in its terms and conditions the grounds on which the ability of business users to offer the same goods and services to consumers under different conditions by means other than through its services may be restricted, or failing to ensure easy access to them by the public;

l) failing to set up an internal complaint-handling system for business users pursuant to Article 11(1) of the Platform-to-Business Regulation;

m) failing to assess or process a complaint or failing to report the outcome of the processing of a complaint pursuant to Article 11(2) of the Platform-Business Relations Regulation;

n) failing to include in its terms and conditions all information on access to its internal complaint-processing system or its functioning pursuant to Article 11(3) of the Platform-Business Relations Regulation;

o) failing, contrary to Article 11(4) of the Platform-Business Relations Regulation, to compile information on the functioning and efficiency of its internal complaint-processing system, to make it easily accessible to the public, to verify it at least once a year or to update it in the event of a significant change;

p) failing to include mediators pursuant to Article 12 of the Platform-to-Business Regulation in its terms and conditions; or

q) failing, contrary to Article 12(6) of the Platform-Business Relations Regulation, to make available to the business user information on the functioning and effectiveness of mediation

relating to its activities.

(2) An internet search engine provider commits an infraction by

a) failing, contrary to Article 5(2), (3) and (5) of the Platform-to-Business Regulation, to establish the main parameters and their relative importance, to provide an easily and publicly accessible description of those parameters in clear and intelligible language in its online search engine or keep that description up to date;

b) failing to allow a corporate website user to become acquainted with the content of the notice pursuant to Article 5(4) of the Platform-Business Relations Regulation; or

c) failing to describe, contrary to Article 7(2) of the Platform-to-Business Regulation, the different treatment it applies or may apply to goods and services offered to consumers through an online search engine either by that provider itself or by corporate website users under its control or by other corporate website users.

(3) For an infraction pursuant to paragraph (1) or (2) a fine of up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

(4) For an infraction pursuant to paragraph (1) or (2) an administrative penalty of publication of the decision on the infraction may be imposed.

§ 50

Infractions committed by providers of intermediary services

(1) A provider of intermediary services commits an infraction by

a) failing to comply with the information obligation pursuant to Article 9(1) or (5) or Article 10(1) or (5) of the Digital Services Regulation;

b) failing to designate a single point of contact pursuant to Article 11(1) or Article 12(1) of the Digital Services Regulation;

c) failing to indicate the official language for communication with its contact point contrary to Article 11(3) of the Digital Services Regulation;

d) breaching the publication obligation pursuant to Article 11(2) or Article 12(2) of the Digital Services Regulation;

e) failing, contrary to Article 13(1) of the Digital Services Regulation. to designate a representative in at least one of the Member States in which it offers services;

f) failing to appoint a representative pursuant to Article 13(2) of the Digital Services Regulation;

g) failing to entrust or provide its representative with powers or means pursuant to Article 13(2) of the Digital Services Regulation;

h) failing, contrary to Article 13(4) of the Digital Services Regulation, to communicate or publish the contact details of its representative to the Office;

i) failing to comply with the information obligation pursuant to Article 14(1) or (2) of the Digital Services Regulation;

j) failing to explain the terms and conditions of the intermediary service in the manner pursuant to Article 14(3) of the Digital Services Regulation;

k) failing to explain the restrictions on the use of the intermediary service in the manner pursuant to Article 14(3) of the Digital Services Regulation;

l) breaching the obligation under Article 14(4) of the Digital Services Regulation when applying or enforcing the restriction;

m) failing to comply with the publication obligation pursuant to Article 15(1) of the Digital Services Regulation;

n) failing to provide the Office or the Office for Personal Data Protection with information on the basis of a request pursuant to § 35(1);

o) failing to allow the Office or the Office for Personal Data Protection to carry out an inspection or failing to provide the necessary cooperation;

p) failing to submit an action plan by the deadline set by the Office or the Office for Personal Data Protection pursuant to § 39(1);

q) failing to comply with an action plan approved by the Office or the Office for Personal Data Protection pursuant to § 39(3)(a);

r) failing to comply with an obligation arising from a corrective measure imposed on him by the Office or the Office for Personal Data Protection pursuant to § 43, or

s) failing to comply with an obligation resulting from a court decision pursuant to the first subparagraph of Article 51(3)(b) of the Digital Services Regulation.

(2) For an infraction pursuant to paragraph (1), a fine may be imposed

a) up to 6% of the offender's annual worldwide turnover for the last completed financial year in the case of the offence pursuant to paragraph (1)(a) to (m) and (p) to (s); or

b) up to 1% of the offender's annual worldwide turnover for the last completed financial year, in the case of an infraction pursuant to paragraph (1)(n) and (o).

§ 51

Infractions committed by hosting service providers

(1) A hosting service provider commits an infraction by

a) failing to establish a notification and action mechanism pursuant to Article 16(1) and (2) of the Digital Services Regulation;

b) failing to send the confirmation pursuant to Article 16(4) of the Digital Services Regulation;

c) failing to settle a notification in the manner pursuant to Article 16(6) of the Digital Services Regulation and, in the case of a notification pursuant to Article 22(8) of Regulation (EU) 2023/988,[11)] failing to settle it without undue delay, at the latest within 3 working days;

d) failing to comply with the information obligation pursuant to Article 16(5) or (6) of the Digital Services Regulation;

e) failing to provide the recipient of the intermediary service concerned with a statement of reasons for the restriction imposed on that recipient pursuant to Article 17 of the Digital Services Regulation; or

f) failing to make a notification pursuant to Article 18 of the Digital Services Regulation.

(2) For an infraction pursuant to paragraph (1) a fine of up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

§ 52

Infractions committed by online platform providers

(1) A provider of an online platform commits an infraction by not communicating to the Office or the Commission information or additional information pursuant to Article 24(3) of the Digital Services Regulation.

(2) A provider of an online platform not exempt under Article 19 of the Digital Services Regulation commits an infraction by

a) failing make available to the recipient the internal complaint-handling system pursuant to Article 20(1) to (3) of the Digital Services Regulation for the purpose of settling his or her complaint;

b) failing to settle the complaint in the manner set out in Article 20(4) to (6) of the Digital Services Regulation;

c) failing to ensure access to information on the possibility for recipients of the service to have access to out-of-court dispute resolution in the manner pursuant to Article 21(1) of the Digital Services Regulation;

d) failing to cooperate with a certified out-of-court dispute resolution body in the manner pursuant to Article 21(2) of the Digital Services Regulation;

[11)] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC.

e) seriously jeopardising the exercise of the activities of a certified out-of-court dispute resolution body by breaching the fee obligation under Article 21(5) of the Digital Services Regulation;

f) failing to take action pursuant to Article 22(1) of the Digital Services Regulation;

g) failing to comply with the obligation to suspend the provision of the service to the recipient pursuant to Article 23(1) of the Digital Services Regulation;

h) failing to suspend the settlement of the notification or complaints contrary to Article 23(2) of the Digital Services Regulation;

i) deciding to suspend the settlement of notices or complaints or the provision of services contrary to Article 23(3) of the Digital Services Regulation;

j) failing to specify its policy with regard to abuse, contrary to Article 23(4) of the Digital Services Regulation;

k) failing to comply with the publication obligation pursuant to Article 24(1) or (2) of the Digital Services Regulation;

l) failing to submit a reasoned decision on restriction to the Commission contrary to Article 24(5) of the Digital Services Regulation;

m) designing, organising or operating its online interface contrary to Article 25 of the Digital Services Regulation;

n) failing to allow the recipient of its service to ascertain the facts of advertising pursuant to Article 26(1) of the Digital Services Regulation in the manner specified therein;

o) failing to provide the recipient of its service with functionality pursuant to the first subparagraph of Article 26(2) of the Digital Services Regulation;

p) failing to ensure, contrary to the second subparagraph of Article 26(2) of the Digital Services Regulation, that the recipient of its service can determine that the content provided by the recipient of its service constitutes or contains commercial communications;

q) presenting advertising to the recipient of their service contrary to of Article 26(3) of the Digital Services Regulation;

r) failing to comply with the information obligation pursuant to Article 27(1) and (2) of the Digital Services Regulation;

s) failing to provide the recipient of its service with a functionality pursuant to Article 27(3) of the Digital Services Regulation;

t) failing to implement measures pursuant to Article 28(1) of the Digital Services Regulation;

u) displaying advertising on its online interface contrary to Article 28(2) of the Digital Services Regulation; or

v) failing to take action pursuant to Article 86(2) of the Digital Services Regulation.

(3) For an infraction pursuant to paragraph (1) and (2) a fine of up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

§ 53

Infractions committed by providers of online platforms allowing consumers to conclude distance contracts with businesses

(1) A provider of an online platform pursuant to Article 30(1) of the Digital Services Regulation not exempt pursuant to Article 29 of this Act commits an infraction by

a) enabling the promotion of communications, offering products or offering services on its online platform to businesses providers from whom it has not received information pursuant to Article 30(1) of the Digital Services Regulation;

b) enabling the promotion of communications, offering products or offering services on its online platform to a business provider from whom it has not received the information pursuant to the second subparagraph of Article 30(2) of the Digital Services Regulation before the expiry of the set deadline;

c) failing to comply with the obligation to assess the reliability and completeness of the information contrary to Article 30(2) of the Digital Services Regulation;

d) failing, contrary to Article 30(2) of the Digital Services Regulation, to make the commencement or continuation of the provision of services of the business subject to an assessment of the reliability and completeness of the information;

e) failing to request corrective action pursuant to the first subparagraph of Article 30(3) of the Digital Services Regulation;

f) failing to suspend the provision of services contrary to the second subparagraph of Article 30(3) of the Digital Services Regulation;

g) failing, contrary to Article 30(4) of the Digital Services Regulation, to allow a business, whose services have been refused or interrupted, to lodge a complaint or to contact a certified out-of-court dispute resolution body;

h) breaching the obligation pursuant to Article 30(5) of the Digital Services Regulation to store the information received from a business;

i) communicating the information received from a business to a third party contrary to Article 30(6) of the Digital Services Regulation;

j) failing to comply with the information obligation pursuant to Article 30(7) of the Digital Services Regulation;

k) operating an online interface that is not designed or arranged in accordance with Article 31(1) or (2) of the Digital Services Regulation, and, in the case of product safety, operating an online interface designed or configured contrary Article 22(9) of Regulation (EU) 2023/988;[11)];

l) failing to comply with the obligation to assess information pursuant to Article 31(3) of the Digital Services Regulation;

m) failing to carry out random verifications pursuant to Article 31(3) of the Digital Services Regulation and, as regards product safety, failing to carry out verifications in accordance with Article 22(7) of Regulation (EU) 2023/988[11)];

n) failing to comply with the information obligation pursuant to Article 32(1) of the Digital Services Regulation; or

o) failing to comply with the publication obligation pursuant to Article 32(2) of the Digital Services Regulation.

(2) For an infraction pursuant to paragraph (1) a fine of up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

§ 54

Infractions committed by internet search engine providers

(1) A provider of an online search engine commits an infraction by failing to communicate to the Office or the Commission information or additional information pursuant to Article 24(3) of the Digital Services Regulation.

(2) An online search engine provider not exempt pursuant to Article 19 of the Digital Services Regulation commits an infraction by failing to comply with the publication obligation pursuant to Article 24(2) of the Digital Services Regulation.

(3) For an infraction, a fine may be imposed up to the amount of

a) 1% of the offender’s annual worldwide turnover for the last completed financial year, in the case of an infraction pursuant to paragraph (1); and

b) 6% of the offender’s annual worldwide turnover for the last completed financial year, in the case of an infraction pursuant to paragraph (2).

§ 55

Infractions of an online short-term rental platform provider

(1) A provider of an online short-term rental platform pursuant to Article 3(5) of Regulation (EU) 2024/1028 of the European Parliament and of the Council on the collection and sharing of data relating to short-term accommodation rental services[12)] commits an infraction by

a) using an online interface that is not designed and configured in the manner pursuant to Article 7(1)(a) or (b) of this Regulation;

[12)] Regulation (EU) 2024/1028 of the European Parliament and of the Council of 11 April 2024 on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724.

b) failing to carry out the checks pursuant to Article 7(1)(c) of this Regulation; or

c) failing to assess the completeness of the host declaration contrary Article 8 of this Regulation.

(2) For an infraction pursuant to paragraph (1) a fine of up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

§ 56

Infractions committed by providers of a very large online platform or a very large online search engine

(1) A provider of a very large online platform or a very large online search engine commits an infraction by

a) failing to provide the recipient with a summary pursuant to Article 14(5) of the Digital Services Regulation; or

b) failing to comply with the publication obligation pursuant to Article 14(6) of the Digital Services Regulation.

(2) For an infraction pursuant to paragraph (1) a fine of up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

§ 57

Infractions committed by persons other than an intermediary service provider

(1) A natural person, a sole trader or a legal entity commits an infraction by unlawfully impersonating a trusted flagger.

(2) Legal entities or sole traders commit an infraction by

a) falsely presents themselves as a certified out-of-court dispute resolution body; or

b) failing to comply with an obligation resulting from a court decision pursuant to point (b) of the first subparagraph of Article 51(3) of the Digital Services Regulation.

(3) A trusted flagger commits an infraction by

a) failing to comply with the obligation to provide information pursuant to § 14(1); or

b) failing to report on notifications pursuant to Article 22(3) of the Digital Services Regulation.

(4) A certified out-of-court dispute resolution body commits an infraction by

a) failing to comply with the obligation to provide information pursuant to § 14(1);

b) performing the activities of a certified out-of-court dispute resolution body without fulfilling the conditions pursuant to Article 21(3) of the Digital Services Regulation;

c) failing to provide a report on functioning pursuant to Article 21(4) of the Digital Services Regulation; or

d) charging a fee contrary to Article 21(5) of the Digital Services Regulation.

(5) A vetted researcher commits and infraction by failing to comply with the obligation to provide information pursuant to § 14(1).

(6) For an infraction, a fine may be imposed up to the amount of

a) CZK 100,000 in the case of an offence pursuant to paragraph (3)(a), paragraph (4)(a) or paragraph (5);

b) CZK 1,000,000 in the case of an infraction pursuant to paragraph (1);

c) CZK 5,000,000 in the case of an infraction pursuant to paragraph (2)(a) or paragraph (4)(b);

d) up to 6% of the offender's annual worldwide turnover for the last completed financial year in the case of an infraction pursuant to paragraph (2)(b), paragraph (3)(b) or paragraph (4)(c) and (d).

§ 58

Infractions committed by providers of data intermediation services

(1) A provider of data intermediation services commits an infraction by

a) providing data intermediation services without submitting a notification pursuant to Article 11(1) prepared in accordance with Article 11(6) of the Data Governance Regulation;

b) failing, contrary to Article 11(3) of the Data Governance Regulation, to designate a representative in at least one of the Member States in which it offers data intermediation services;

c) improper use of a designation or logo pursuant to Article 11(9) of the Data Governance Regulation;

d) failing to notify the Office pursuant to Article 11(12) of the Data Governance Regulation;

e) failing, contrary to Article 11(13) of the Data Governance Regulation, to notify the Office of the termination of the data intermediation activity;

f) using the data for which it provides data intermediation services contrary to Article 12(a) of the Data Governance Regulation;

g) failing provide data intermediation services through a separate legal entity contrary to Article 12(a) of the Data Governance Regulation;

h) making the commercial terms and conditions of the provision of data intermediation services conditional on the use of another service contrary to Article 12(b) of the Data Governance Regulation;

i) using data contrary to Article 12(c) of the Data Governance Regulation;

j) failing to make data available at the request of the data holder pursuant to Article 12(c) of the Data Governance Regulation;

k) converting data into a specific format contrary to Article 12(d) of the Data Governance Regulation;

l) failing to offer the data subject or data holder the possibility of an exemption pursuant to Article 12(d) of the Data Governance Regulation;

m) failing to provide access to its data intermediation service in the manner set out in Article 12(f) of the Data Governance Regulation;

n) failing to implement the procedures pursuant to Article 12(g) of the Data Governance Regulation;

o) failing to ensure, contrary to Article 12(h) of the Data Governance Regulation, adequate continuity in the provision of data intermediation services in the event of its insolvency;

p) failing to put in place mechanisms allowing access to retained data pursuant to Article 12(h) of the Data Governance Regulation;

q) failing to take appropriate measures to ensure interoperability contrary to Article 12(i) of the Data Governance Regulation;

r) failing to implement measures pursuant to Article 12(j) of the Data Governance Regulation;

s) failing to comply with the information obligation pursuant to Article 12(k) of the Data Governance Regulation;

t) failing to take action pursuant to Article 12(l) of the Data Governance Regulation;

u) failing to ensure the required level of security of competition-sensitive information pursuant to Article 12(l) of the Data Governance Regulation;

v) breaching the obligation to act in the best interest of the data subject pursuant to Article 12(m) of the Data Governance Regulation;

w) fails to specify, contrary to Article 12(n) of the Data Governance Regulation, the jurisdiction of the third State in which the data are to be used;

x) failing to provide, contrary to Article 12(n) of the Data Governance Regulation, tools for granting and withdrawing consent to data subjects or for granting and withdrawing consent for data processing to data holders; or

y) failing keep, contrary to Article 12(o) of the Data Governance Regulation, records of data intermediation activity.

(2) For an infraction pursuant to paragraph (1) a fine of up to CZK 10,000,000 or up to 6% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

(3) An infraction pursuant to paragraph (1) may be subject to an administrative penalty of prohibition of activity for up to one year.

§ 59

Infractions committed by recognised data altruism organisations

(1) A recognised data altruism organisation commits an infraction by:

a) failing to designate a representative, contrary to Article 19(3) of the Data Governance Regulation, in at least one of the Member States in which it offers data altruism services;

b) failing to notify the Office pursuant to Article 19(7) of the Data Governance Regulation;

c) failing to keep records of facts pursuant to Article 20(1) of the Data Governance Regulation;

d) failing to prepare or transmit an annual activity report to the Office pursuant to Article 20(2) of the Data Governance Regulation;

e) failing to comply with the information obligation pursuant to Article 21(1) of the Data Governance Regulation;

f) using data contrary to Article 21(2) of the Data Governance Regulation;

g) using misleading marketing practices when requesting the provision of data pursuant to Article 21(2) of the Data Governance Regulation;

h) failing to provide the necessary tools for granting consent and its easy withdrawal pursuant to Article 21(3) of the Data Governance Regulation;

i) failing to take measures ensuring an adequate level of security pursuant to Article 21(4) of the Data Governance Regulation;

j) failing to comply with the information obligation pursuant to Article 21(5) of the Data Governance Regulation;

k) failing to specify, contrary to Article 21(6) of the Data Governance Regulation, the jurisdiction of the third State in which the data are to be used.

(2) For an infraction pursuant to paragraph (1) a fine of up to CZK 1,000,000 or up to 1% of the offender's annual worldwide turnover for the last completed financial year may be imposed.

(3) An infraction pursuant to paragraph (1) may be subject to an administrative penalty of prohibition of activity for up to one year.

§ 60

Other infractions related to the status of a recognised data altruism organisation

(1) A natural person, a sole trader or a corporate entity commits an infraction by

a) providing false or incomplete information in the request pursuant to Article 19(1), (2) or (3) of the Data Governance Regulation; or

b) using a designation or logo without authorisation pursuant to Article 17(2) of the Data Governance Regulation.

(2) A fine of up to CZK 1,000,000 may be imposed for an infraction pursuant to paragraph (1).

§ 61

Common infractions of providers of data intermediation services or recognised data altruism organisations

(1) A provider of data intermediation services or a recognised data altruism organisation commits an infraction by

a) failing to take measures to prevent the transfer of non-personal data from the European Union to third countries or to prevent international governmental access pursuant to Article 31(1) of the Data Governance Regulation;

b) transferring data that are not personal data or providing international governmental access to such data contrary Article 31 of the Data Governance Regulation; or

c) failing to comply with the information obligation pursuant to Article 31(5) of the Data Governance Regulation.

(2) For an infraction pursuant to paragraph (1), a fine may be imposed of up to

a) CZK 5,000,000 in the case of an infraction pursuant to paragraph 1(c);

b) CZK 10,000,000 in the case of an infraction pursuant to paragraph (1)(a) and (b).

(3) An infraction pursuant to paragraph (1) may be subject to an administrative penalty of prohibition of activity for up to one year.

§ 62

Infractions in the field of confidentiality, information obligations and general prohibitions

(1) A natural person, legal entity or sole trader involved in the supervision of compliance with the Digital Services Regulation, the Data Governance Regulation, except for the re-use of data held

by public sector bodies, the Platform-Business Regulation or in providing cooperation pursuant to § 31 commits an infraction by breaching the confidentiality obligation pursuant to § 34.

(2) Legal entities or sole traders who are not providers of intermediary services commit and infraction by

a) failing to provide the Office or the Office for Personal Data Protection with complete or true information on the basis of a request pursuant to § 35(1); or

b) failing to allow the Office or the Office for Personal Data Protection to carry out an inspection or failing to provide the necessary cooperation.

(3) For an infraction, a fine may be imposed up to the amount of

a) CZK 1,000,000 in the case of an infraction pursuant to paragraph (1);

b) 1% of the offender's annual worldwide turnover for the last completed financial year, in the case of an infraction pursuant to paragraph (2).

Section 3
Common provision for dealing with infractions

§ 63
Common provisions concerning infractions

(1) Infractions pursuant to § 49, § 50(1)(a) to (m), § 51, § 52(1) and (2)(a) to (m), (r) to (t) and (v), § 53 to § 56, § 57(1), § 57(2)(a), § 57(3) to (5) and §§ 58 to 61 shall be dealt with by the Office.

(2) Infractions pursuant to § 48(1) to (3) and § 52(2)(n) to (q) and (u) shall be dealt with by the Office for Personal Data Protection.

(3) The administrative authority competent to deal with infractions pursuant to § 50(1)(n) to (s), § 57(2)(b) and § 62(2) shall be the authority responsible for exercising supervision.

(4) An administrative authority shall be competent to deal with an infractions pursuant to § 62(1) in relation to whose competence in the field of supervision or cooperation the confidentiality obligation under § 34 has been breached.

(5) Infractions pursuant to § 48(4) shall be dealt with by a professional chamber with compulsory membership, of which the offender is a member.

(6) Revenue from fines shall be revenue of the budget used for financing the activities of the authority that imposed the fine. The Office collects and enforces fines it has imposed.

(7) The limitation period is 3 years. If the limitation period has been interrupted, liability for the infraction shall lapse at latest 5 years after the infraction was committed.

Section 4
Coercive fines

§ 64
Distraint of benefits in kind

(1) When executing distraint on benefits in kind against persons set out in Article 51(1)(a) of the Digital Services Regulation, for an obligation imposed on the basis of the Digital Services Regulation, a coercive fine may be imposed for each day of delay in complying with the obligation up to the date of the decision imposing the coercive fine, up to the amount of

a) 5% of the average daily worldwide turnover of the fined entity for the last completed financial year, if an accounting unit is involved; or

b) 5% of the average daily worldwide income of the fined entity for the last completed financial year, if an accounting unit is not involved.

(2) The aggregate upper limit of repeatedly imposed coercive fines stipulated by the Administrative Code shall not apply in the cases pursuant to paragraph (1).

Title VIII
Common, transitional and repealing provisions

§ 65
Common provisions

(1) In proceedings pursuant to Title VI or VII, the provisions of the Code of Administrative Procedure on the possible method of terminating appeal proceedings shall not apply.

(2) § 42 of the Code of Administrative Procedure applies to the procedure for settling a complaint pursuant to Article 53 of the Digital Services Regulation or Article 27 of the Data Governance Regulation, unless otherwise provided for in the Digital Services Regulation or the Data Governance Regulation.

§ 66
Transitional provisions

(1) Proceedings pursuant to the Act governing certain information society services[13)] that have not been definitively terminated before the effective date of this Act shall be completed in accordance with existing legislation.

(2) The period pursuant to § 9(1)(c) shall expire at the earliest 24 months after the effective date of this Act.

[13)] Act No 480/2004 on certain information society services and amending certain acts, as amended.

§ 67

Repealing provisions

The following are repealed:

1. Act No 480/2004 on certain information society services and amending certain acts (the Act on Certain Information Society Services).

2. Part Forty-Six of Act No 444/2005 amending Act No 531/1990 on territorial financial authorities, as amended and some related acts.

3. Part Eight of Act No 214/2006 amending Act No 455/1991 on trade licensing (the Trade Licensing Act), as amended, and certain other acts.

4. Part Six of Act No 160/2007 amending certain laws in the field of consumer protection.

5. Part One Hundred and Forty-Five of Act No 281/2009 amending certain acts in connection with the adoption of the Tax Code.

6. Part Eighty-Eight of Act No 375/2011 amending certain acts in connection with the adoption of the Health Services Act, the Specific Health Services Act, and the Emergency Medical Service Act.

7. Part Two of Act No 468/2011 amending Act No 127/2005 on electronic communications and amending certain related acts (the Electronic Communications Act), as amended, and certain other acts.

8. Part One Hundred and Fifty-Eight of Act No 183/2017 amending certain acts in connection with the adoption of the Act on Liability and Proceedings for Offences and the Act on Certain Infractions.

9. Part Seven of Act No 238/2020 amending Act No 634/1992 on consumer protection, as amended, and other related acts.

10. Act No 58/2023 amending Act No 480/2004 on certain information society services and amending certain acts (the Act on Certain Information Society Services), as amended.

PART TWO

§ 68

Amendment to the Criminal Procedure Code

In Act No 141/1961, on Criminal Court Proceedings (the Criminal Procedure Code), as amended by Act No 57/1965, Act No 58/1969, Act No 149/1969, Act No 48/1973, Act No 29/1978, Act No 43/1980, Act No 159/1989, Act No 178/1990, Act No 303/1990, Act No 558/1991, Act No 25/1993, Act No 115/1993, Act No 292/1993, Act No 154/1994, Constitutional Court ruling promulgated under No 214/1994, Constitutional Court ruling promulgated under No 8/1995, Act No 152/1995, Act No 150/1997, Act No 209/1997, Act No 148/1998, Act No 166/1998, Act No 191/1999, Act No 29/2000, Act No 30/2000, Act No 227/2000, Constitutional Court ruling promulgated under No 77/2001, Act No 144/2001, Act No 265/2001, Constitutional Court ruling

promulgated under No 424/2001, Act No 200/2002, Act No 226/2002, Act No 320/2002, Act No 218/2003, Act No 279/2003, Act No 237/2004, Act No 257/2004, Act No 283/2004, Act No 539/2004, Act No 587/2004, Constitutional Court ruling promulgated under No 45/2005, Constitutional Court ruling promulgated under No 239/2005, Act No 394/2005, Act No 413/2005, Act No 79/2006, Act No 112/2006, Act No 113/2006, Act No 115/2006, Act No 165/2006, Act No 253/2006, Act No 321/2006, Act No 170/2007, Act No 179/2007, Act No 345/2007, Constitutional Court ruling promulgated under No 90/2008, Act No 121/2008, Act No 129/2008, Act No 135/2008, Act No 177/2008, Act No 274/2008, Act No 301/2008, Act No 384/2008, Act No 457/2008, Act No 480/2008, Act No 7/2009, Act No 41/2009, Act No 52/2009, Act No 218/2009, Act No 272/2009, Act No 306/2009, Constitutional Court ruling promulgated under No 163/2010, Act No 197/2010, Constitutional Court ruling promulgated under No 219/2010, Act No 150/2011, Act No 181/2011, Act No 207/2011, Act No 330/2011, Act No 341/2011, Act No 348/2011, Act No 357/2011, Act No 459/2011, Constitutional Court ruling promulgated under No 43/2012, Act No 193/2012, Act No 273/2012, Act No 390/2012, Act No 45/2013, Act No 105/2013, Act No 141/2014, Act No 77/2015, Act No 86/2015, Act No 150/2016, Act No 163/2016, Act No 243/2016, Act No 264/2016, Act No 298/2016, Act No 301/2016, Act No 455/2016, Act No 55/2017, Act No 56/2017, Act No 57/2017, Act No 58/2017, Act No 59/2017, Act No 183/2017, Act No 204/2017, Act No 178/2018, Act No 287/2018, Act No 111/2019, Act No 203/2019, Act No 255/2019, Act No 315/2019, Act No 114/2020, Act No 165/2020, Act No 333/2020, Act No 220/2021, Act No 418/2021, Act No 130/2022, Act No 422/2022, Act No 173/2023, Act No 326/2023, Act No 349/2023, Act No 29/2024, Act No 165/2024, Act No 166/2024, Act No .../2024 and Act No .../2024, a new § 8e is inserted after § 8d, which reads as follows, including the heading and footnote No 15:

‘§ 8e

Cooperation and provision of information pursuant to the Digital Services Regulation

(1) The order set out Article 9(1) of Regulation (EU) 2022/2065 of the European Parliament and of the Council[15)] (hereinafter the 'Digital Services Regulation') that is sent by a law enforcement authority to a provider of intermediary services must meet the requirements set out in Article 9(2)(a) of the Digital Services Regulation, the condition set out in Article 9(2)(b) of the Digital Services Regulation, and must be sent in the language specified in Article 9(2)(c) of the Digital Services Regulation, to the extent set out in this Article.

(2) The order set out in Article 10(1) of the Digital Services Regulation that is sent by a law enforcement authority to a provider of intermediary services must comply with the requirements set out in Article 10(2)(a)(i) to (iv) and (vi) of the Digital Services Regulation and the condition set out in Article 10(2)(b) of the Digital Services Regulation, and must be sent in the language specified in Article 10(2)(c) of the Digital Services Regulation to the extent set out in this Article. The order pursuant to Article 10(1) of the Digital Services Regulation may be sent to a provider of intermediary services without justification if sending it would jeopardise the prevention, investigation, or prosecution of criminal offences.

(3) An order pursuant to Article 9 or Article 10 of the Digital Services Regulation shall be sent to the electronic contact point in accordance with Article 11 of the Digital Services Regulation; this does not apply if

a) the order contains information classified under the Act governing the protection of classified information;

b) another way of transmitting the order requires the protection of the confidentiality of the criminal proceedings or the privacy of the persons involved; or

c) a faster and more efficient way of transmitting the order is in place with the provider of intermediary services.

(4) A provider of intermediary services that has provided information pursuant to Article 10(1) of the Digital Services Regulation to a law enforcement authority shall not disclose the information pursuant to Article 10(5) of that Act if this Act provides for an information obligation to law enforcement authorities. In other cases, it may do so only with the prior consent of the law enforcement authority conducting the criminal proceedings or by whose decision the criminal proceedings have been finally concluded; If the criminal proceedings have ended at the stage of the proceedings before the court, the consent shall be given by the presiding judge of the court of first instance. Consent cannot be given if the identity of the recipient of the service is not known or if the provision of the information would jeopardise the purpose of the criminal proceedings; the specific reason for non-consent is not disclosed to providers of intermediary services. The law enforcement authority shall inform the intermediary service provider thereof when sending the order set out in Article 10(1) of the Digital Services Regulation.

(5) If a law enforcement authority pursuant to paragraph (4) has given its consent to the provision of information pursuant to Article 10(5) of the Digital Services Regulation, it shall also indicate what remedies are permitted under this Act.

(6) An order issued by a law enforcement authority pursuant to Article 9(1) or Article 10(1) of the Digital Services Regulation shall not be transmitted to the Digital Services Coordinator.

[15)] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation).

PART THREE

§ 69
Amendment of the Act on Consumer Protection

Act No 634/1992 on consumer protection, as amended by Act No 217/1993, Act No 40/1995, Act No 104/1995, Act No 110/1997, Act No 356/1999, Act No 64/2000, Act No 145/2000, Act No 258/2000, Act No 102/2001, Act No 452/2001, Act No 477/2001, Act No 151/2002, Act No 320/2002, Act No 227/2003, Act No 277/2003, Act No 439/2003, Act No 119/2004, Act No 186/2004, Act No 217/2004, Act No 444/2005, Act No 229/2006, Act No 36/2008, Act No 227/2009, Act No 281/2009, Act No 285/2009, Act No 298/2009, Act No 301/2009, Act No 155/2010, Act No 28/2011, Act No 139/2011, Act No 211/2011, Act No 219/2011, Act No 468/2011, Act No 221/2012, Act No 238/2012, Act No 303/2013, Act No 476/2013, Act No 356/2014, Act No 378/2015, Act No 188/2016, Act No 183/2017, Act No 264/2017, Act No 371/2017, Act No 179/2019, Act No 164/2020, Act No 205/2020, Act No 238/2020, Act No 374/2022, Act No 303/2023, Act No 412/2023, Act No 124/2024, Act No 180/2024, and Act No .../2024 are amended as follows:

1. In § 23(2), at the beginning of subparagraph (a), the words ‘§§ 1784a to 1784d, in the case of obligations towards consumers,’ are inserted and the numbers ‘1826,’ and ‘1827,’ are deleted.

2. In the introductory part of § 23a(1), §23a(2), § 23b(2) and (3), and § 23d, the words ‘§§ 1784a to 1784d, in the case of obligations towards consumers,’ are inserted after the words ‘the Act and obligations laid down in,’ and the numbers ‘1826,’ and ‘1827,’ are deleted.

3. In § 24(15)(h), the words ‘with the consumer’ are inserted after the word ‘funds’ and the text ‘§ 1826(1)’ is replaced by ‘§ 1784a’.

4. In § 24(15)(i), the text ‘§ 1826(2)’ is replaced by ‘§ 1784c(1)’.

5. In § 24(15)(l), the text ‘§ 1827(1)’ is replaced by ‘§ 1784c(2)’ and the words ‘to the consumer’ are inserted after the words ‘does not confirm’.

6. In § 24(15)(m), the text ‘§ 1827(2)’ is replaced by ‘§ 1784b’ and the words ‘text of general’ are replaced by ‘content of the contract, including’.

7. In § 24i(2), the words ‘legislation governing certain information society services[57)]’ are replaced by ‘the Digital Economy Act[57)]’.

   Footnote 57 reads as follows:
   ‘[57)] Act No .../2024 on the digital economy and amending certain related acts.’.

8. In Annex 2(c), the words ‘Act No 480/2004’ are replaced by the words ‘Act No .../2024’.

9. In Annex 3, the item on the competence of the supervisory authority of the Office for Personal Data Protection reads as follows:
   ‘

Office for Personal Data Protection	4. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1)	Act No .../2024 on the digital economy and amending certain related acts, as regards the provision of information society services and the dissemination of commercial communications.

	6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37): Article 13	Act No 127/2005 on electronic communications and amending certain related acts in the area of unsolicited communications
		Act No .../2024 on the digital economy and amending certain related acts, as regards the provision of information society services and the dissemination of commercial communications.
	9. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) (OJ L 149, 11.6.2005, p. 22)	Act No 634/1992 on consumer protection, for unsolicited advertising disseminated by electronic means, if the method of dissemination is an unfair commercial practice.
		Act No 40/1995 on the regulation of advertising and amending Act No 468/1991 on the operation of radio and television broadcasting, as amended, in the area of unsolicited advertising disseminated by electronic means, if the method of dissemination is an unfair commercial practice.

’.

PART FOUR

§ 70

Amendment to the Copyright Act

In § 47(5) of Act No 121/2000 on copyright, on rights related to copyright and amending certain acts (the Copyright Act), as amended by Act No 429/2022, the words ‘the Act on Certain Information Society Services[36)]’ are replaced by ‘Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation)[36)]’.

Footnote 36 reads as follows:

’[36)] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).’.

PART FIVE

§ 71

Amendment of the Act on the Czech Agricultural and Food Inspection Authority

Act No 146/2002 on the Czech Agricultural and Food Inspection Authority and amending certain related acts, as amended by Act No 94/2004, Act No 316/2004, Act No 321/2004, Act No 444/2005, Act No 120/2008, Act No 281/2009, Act No 291/2009, Act No 407/2012, Act No 308/2013, Act No 138/2014, Act No 250/2014, Act No 180/2016, Act No 243/2016, Act No 26/2017, Act No 65/2017, Act No 183/2017, Act No 302/2017, Act No 238/2020, Act No 174/2021, Act No 261/2021, Act No 244/2022, Act No 247/2022 and Act No 167/2023 is amended as follows:

1. In § 3(4)(f), the word ‘and’ is replaced by a semicolon, the full stop at the end of subparagraph (g) is replaced by ‘and’ and the following subparagraph (h) is added:

‘h) decides on the imposition of measures on the provider of an intermediary service pursuant to Article 3(g) of Regulation (EU) 2022/2065 of the European Parliament and of the Council hereinafter (the “Digital Services Regulation”).’

2. The following Articles 4d to 4f are inserted after Article 4c:

‘§ 4d

(1) If the intermediation service pursuant to Article 3(g) of the Digital Services Regulation infringes the requirements of the legislation on food, psychomodulatory substances, and scheduled psychoactive substances for which the inspection body is competent, the Inspection Authority shall, as a first step in the proceedings, impose measures on the provider of that intermediation service to

a) remove specific illegal content from its online interface;

b) disable access to an offer containing illegal content on its online interface; or

c) display an explicit warning to consumers about illegal content.

(2) The decision to impose measures pursuant to paragraph (1) must comply with the requirements pursuant to Article 9(2) of the Digital Services Regulation and its operative part must contain

a) information necessary to identify illegal content, such as the exact internet address;

b) the possible corrective measures available to the provider of the intermediary service pursuant to Article 3(g) of the Digital Services Regulation and the person who provided the content; and

c) indication of the supervisory authority or other administrative authority to which the provider of the intermediary service is required to send information on how the measure has been complied with.

§ 4e

(1) If necessary and proportionate for the purpose of identifying persons using an intermediation service pursuant to Article 3(g) of the Digital Services Regulation, who are suspected of infringing the requirements laid down in legislation concerning food, psychomodulatory substances, and scheduled psychoactive substances for which the inspection is competent, the Inspection Authority shall, as the first procedural step, oblige the provider of that intermediation service to provide information on that person.

(2) The decision to impose measures pursuant to paragraph (1) must comply with the requirements pursuant to Article 10(2) of the Digital Services Regulation and its operative part must contain

a) information needed to identify the person using the intermediary service pursuant to Article 3(g) of the Digital Services Regulation, such as their user account name or unique identifier;

b) the possible corrective measures available to the provider of the intermediary service and the person whose information is to be provided;

c) indication of the supervisory authority or other administrative authority to which the provider of the intermediary service is required to send information on how the measure has been complied with.

§ 4f

(1) The Inspection Authority shall notify the provider of an intermediary service pursuant to Article 3(g) of the Digital Services Regulation of the decision imposing measures pursuant to § 4d(1) and § 4e(1) through the one-stop shop pursuant to Article 11 of the same Act. The measure shall be deemed to have been notified on the date on which it is made available to that intermediary service provider in the manner pursuant to the first sentence.

(2) An appeal that does not have suspensory effect may be brought against a decision imposing measures pursuant to § 4d(1) or § 4e(1).’.

§ 72

Technical regulation

This Act was notified in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

PART SIX

§ 72
Amendment to the Administrative Fees Act

In item 109 of the Annex to Act No 634/2004 on administrative fees, as amended by Act No 361/2005, the following points (c) to (g) are added, including footnotes 87 and 88:

‘c) Receipt of a request for the issuance of a certificate pursuant to Article 11(8) of the Data Governance Regulation[88)] CZK 1000
d) Receipt of a request for the issuance of a certificate pursuant to Article 11(9) of the Data Governance Regulation[88)] CZK 10,000

e) Receipt of an application for a certification decision pursuant to Article 21(3) of the Digital Services Regulation[89)]
CZK 10,000

f) Receipt of an application for a decision granting the status of trusted flagger pursuant to Article 22(2) of the Digital Services Regulation[89)] CZK 10,000

g) Receipt of an application for a decision granting the status of vetted researcher pursuant to Article 40(8) of the Digital Services Regulation[89)] CZK 1000

[88)] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation).

[89)] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation).

PART SEVEN

§ 73
Amendment to the Act on on-demand audiovisual media services

In § 18 of Act No 132/2010 on on-demand audiovisual media services and amending certain acts (the Act on on-demand audiovisual media services), the words ‘No 480/2004 on certain information society services and amending certain acts (the Act on certain information society services), as amended’ are replaced by the words ‘on the digital economy[2)]’.

Footnote 2 reads as follows:

‘[2)] Act No .../2024 on the digital economy and amending certain related acts.’.

PART EIGHT

§ 74
Amendment of the Civil Code

Act No 89/2012, the Civil Code, as amended by Act No 460/2016, Act No 303/2017, Act No 111/2018, Act No 171/2018, Act No 163/2020, Act No 33/2020, Act No 192/2021, Act No 429/2022, Act No 374/2022, Act No 414/2023, Act No 31/2024, Act No 123/2024, Constitutional Court ruling No 144/2024, Act No .../2024 and Act No .../2024, is amended as follows:

1. The following Section 1784a to Section 1784d are inserted after Section 1784 which, including their header, read as follows:

E-commerce

§ 1784a

A business using electronic means to conclude a contract shall inform the other party in a clear and comprehensible manner, before the latter places the order, of

a) individual technical steps leading to the conclusion of the contract,

b) whether a copy of the concluded contract will be deposited with him or her and whether he or she will allow access to it;

c) options as regards detecting and correcting errors made when entering data before placing an order;

d) details of the languages in which the contract may be concluded; and

e) an indication of the code of conduct, if the business has undertaken to comply with it, and an indication of how its content can be accessed electronically.

§ 1784b

The business shall acquaint the other party in text form with the content of the contract, including the terms and conditions.

§ 1784c

(1) Before placing an order, the business shall allow the other party to check and amend the data provided in the order.

(2) The business shall confirm the receipt of the order by electronic means to the other party without undue delay.

§ 1784d

(1) The provisions of § 1784a and § 1784c shall not apply if the contract is concluded exclusively by exchange of email or similar individual communication.

(2) If the other party is a consumer, provisions derogating from § 1784a to § 1784c to the detriment of the consumer shall be ignored.’.

2. § 1826 and § 1827 are deleted.

PART NINE
§ 75
Amendment to the Act on special judicial proceedings

Act No 292/2013 on Special Judicial Proceedings, as amended by Act No 87/2015, Act No 161/2016, Act No 189/2016, Act No 298/2016, Act No 334/2016, Act No 460/2016, Act No 296/2017, Act No 303/2017, Act No 343/2020, Act No 527/2020, Act No 588/2020, Act No 192/2021, Act No 363/2021, Act No 285/2023, Act No 349/2023, Act No 414/2023, Act No .../2024 and Act No .../2024, is amended as follows:

1. In § 2(j), the words ‘in matters relating to the protection of competition’ are replaced by the words ‘or inspections (hereinafter "investigations")’.

2. In § 2, the following subparagraph (p) is inserted after subparagraph (o):
’(p) on the temporary restriction of access to an intermediation service;’.

Subparagraphs (p) to (u) become subparagraphs (q) to (v).

3. In § 3(2)(g), the words ‘in matters relating to the protection of competition’ are deleted.

4. In § 22a, the words ‘records in the Register’ are replaced by ‘Register’.

5. In Title IV of Part Two, in the heading of Section 4, the words ‘in matters of economic competition’ are deleted.

6. § 323, including heading, reads as follows:

‘§ 323
Territorial jurisdiction

The competent court is,

a) for proceedings in matters of the protection of competition, the court in whose district the Office for the Protection of Competition has its seat;

b) for proceedings in matters of the digital economy, the court in whose district the Czech Telecommunication Office has its seat.

7. § 324, including heading, reads as follows:

‘§ 324
Subject matter of the proceedings

In proceedings, the court shall decide whether to consent to an investigation if there is a reasonable suspicion that business books or other records related to the subject matter of the investigation are located in premises other than the business premises of the person under investigation, including the flats of natural persons who are members of the statutory bodies or employees of the person under investigation, or other dwellings of such persons that are not used for business or other economic activities (hereinafter “other than business premises”), and if such an investigation is to be carried out on those premises.’.

8. § 325(1) reads as follows:

‘(1) Proceedings may be initiated

a) in matters of competition only to a motion of the Office for the Protection of Competition or the European Commission;

b) in matters of the digital economy, only on a motion of the Czech Telecommunication Office, the Office for Personal Data Protection or the European Commission.’.

9. In § 326, the last sentence is deleted.

10. The existing text of § 326 becomes paragraph (1) and the following paragraph (2) is added:

‘(2) If the applicant is the European Commission,

a) the Office for the Protection of Competition is also a participant in matters of protection of competition;

b) the Office for Personal Data Protection is also a participant in matters of the digital economy, if the Office for Personal Data Protection would otherwise be competent to submit a proposal, otherwise the Czech Telecommunication Office is a participant.’.

11. In Title IV of Part Two, a new § 10 is inserted after § 9, including the heading and footnote 10, and reads as follows:

'Section 10
Proceedings for the temporary restriction of access to an intermediary service

§ 366a
Territorial jurisdiction

For proceedings on the temporary restriction of access to an intermediary service under directly applicable European Union legislation on the single market for digital services[11)], the general court of the applicant has jurisdiction.

§ 366b

Initiation of proceedings

(1) Proceedings may be initiated only at the request of the Czech Telecommunication Office or the Office for Personal Data Protection.

(2) In addition to the general requirements of the proposal, the proposal must contain

a) an indication of whether the proposal is submitted at the request of the European Commission; and

b) an indication of whether the applicant should be authorised by the court to extend the duration of the restriction on access to the intermediation service, and, where appropriate, an indication of how many extensions should be authorised by the court and on what grounds it is requested.

§ 366c

Participants

(1) Participants are

a) the applicant;

b) the provider of the intermediary service to which access is to be restricted; and

c) the intended addressee of the proposed measures, with the exception of the provider of the internet access service.

(2) A participant is also

a) the provider of an internet access service who, as a result of the court's decision, is required by the application to temporarily restrict access to the website and who informs the court within the period pursuant to § 366e(2) that he is intervening in the proceedings; and

b) a party that informs the court within the period pursuant to § 366e(2) that they are entering the proceedings as an additional party and at the same time demonstrates a legitimate interest in the subject matter of the proceedings or their outcome.

§ 366d

Rejection of the motion

A motion that does not contain all essentials or that is incomprehensible or vague shall be rejected by the court if it is not possible to continue the proceedings because of these deficiencies; a provision on rectification or completion of a submission which does not contain all the requisites or which is incomprehensible or indeterminate shall not apply. The court shall also reject the motion if it was submitted by someone who is not entitled to submit it.

§ 366e

Proceedings

(1) If the court has not acted in accordance with § 366d, it shall issue a ruling stating that proceedings for the temporary restriction of access to the intermediation service have been initiated, as well as the cases concerned by those proceedings, and that the persons pursuant to § 366c(2) have the right to intervene in the proceedings as an additional party. This ruling shall be posted on the court's notice board.

(2) The deadline for exercising the right to intervene as an additional party is 7 days from the date of posting of the order on the court notice board; the court must inform the parties of this in the ruling.

§ 366f
Hearing

A hearing does not need to be ordered.

§ 366g
Taking of evidence

In proceedings, the court may take evidence other than that proposed by the parties only if it is necessary to establish the facts and if it results from the content of the dossier. § 11, § 17, § 20(1) to (3), § 21 and § 28 shall not apply.

§ 366h
Decision and its effects

(1) The court shall rule on the motion as a matter of priority.

(2) A decision approving the motion is enforceable

a) 5 days after the date of registration of the website subject to the temporary restriction in the list of services with temporarily restricted access under the Digital Economy Act, in the case of a decision granting a proposal for a temporary restriction on access to the website to be implemented by the internet access service provider; or

b) after 3 days have passed from the date it was posted on the official notice board of the court in other cases.

§ 366i
Delivery

(1) The court delivers documents to the provider of intermediary services

a) through the contact point pursuant to directly applicable European Union legislation on the Single Market for Digital Services; a document is deemed to have been delivered after the end of the tenth day from the date of its dispatch;

b) via the public data network to a data mailbox, if the document cannot be served in the manner pursuant to (a); or

c) by posting it on the court notice board, if the provider of intermediary services does not have a data mailbox available.

(2) The court delivers documents to parties pursuant to § 366c(2)(b) by posting them on the court's official notice board.

(3) The decision granting the motion to temporarily restrict access to the website, to be implemented by the provider of the internet access service, must also be served on the authority that maintains the list of services with temporarily restricted access under the Digital Economy Act.

§ 366j
Appeals

An appeal has no suspensive effect.

[11)] Article 51(3) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation).

PART TEN

§ 76
Amendment to the Cybersecurity Act

In § 2(l) of the introductory part of Act No 181/2014 on cyber security and amending related acts (the Cybersecurity Act), as amended by Act No 205/2017, the words 'regulating certain information society services'[9)]' are replaced by the words 'on the digital economy[9)]'.

Footnote 9 reads as follows:
'[9)] Act No .../2024 on the digital economy and amending certain related acts.'.

PART ELEVEN
EFFECTIVE DATE

§ 77

This Act shall take effect on the fifteenth day following its promulgation, with the exception of the provisions of

a) § 18(3), which shall take effect on the day following its promulgation; and

b) § 13(1), 14(2), 19, and 21(1), which shall take effect on 1 July 2025.