Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:

10 November 2005 [shall come into force on 14 December 2005];

12 June 2009 [shall come into force on 1 July 2009];

19 May 2011 [shall come into force on 8 June 2011];

23 November 2020 [shall come into force on 1 January 2021];

27 April 2023 [shall come into force on 29 May 2023];

23 May 2024 [shall come into force on 21 June 2024].

If a whole or part of a section has been amended, the date of the amending law appears in square brackets at the end of the section. If a whole section, paragraph or clause has been deleted, the date of the deletion appears in square brackets beside the deleted section, paragraph or clause.

The *Saeima 1*  has adopted and

the President has proclaimed the following law:

**Law on Information Society Services**

**Chapter I. General Provisions**

**Section 1. Terms Used in the Law**

(1) The following terms are used in the Law:

1) **electronic mail** – a type of services which ensures the possibility for computer users connected to an electronic communications network to send and receive a notification;

2) **information society service** – a distance service (parties do not meet simultaneously) which is usually a paid service provided using electronic means (electronic information processing and storage equipment, including digital compression equipment) and upon individual request of a service recipient. Information society services include the electronic trade of goods and services, sending commercial communications, offering possibilities for searching for information, access thereto, and obtaining the information, services that ensure the transmission of information in an electronic communications network or access to an electronic communications network, and storage of information, and also online intermediation platform services;

3) **commercial communication** – any form of communication in electronic form designed to directly or indirectly advertise the goods or services or to advertise the image of a merchant, organisation, or person pursuing a commercial, industrial, or craft activity or a regulated profession. Information allowing direct access to general information about the service provider and the activities thereof (domain name or electronic mail address) shall not be regarded as a commercial communication;

4) **co-ordinated field** – area in which the procedures for the provision of information society services (requirements for the commencement and performance of commercial activities), and also the requirements for information society services specified in laws and regulation are in effect. The co-ordinated field does not include requirements for goods or their delivery;

5) [23 May 2024];

6) **hosting service provider** – a provider of information society services which ensures the storage of the information provided by a content provider upon request of the content provider.

(2) Terms used in the Law:

1) “subscriber”, “user”, and “terminal equipment” corresponds to the terms used in the Electronic Communications Law;

2) “association” and “foundation” corresponds to the terms “organisation” and “association” used in 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 (hereinafter – Regulation No 2019/1150);

3) “business user” corresponds to the term used in Regulation No 2019/1150;

4) “corporate website user” corresponds to the term “corporate website user” used in Regulation No 2019/1150;

5) “provider of online intermediation platform services” corresponds to the term “provider of online intermediation services” used in Regulation No 2019/1150;

6) “content provider” corresponds to the term used in Article 2(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (hereinafter – Regulation No 2021/784);

7) “intermediary service” corresponds to the term used in Article 3(g) 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 Act) (hereinafter – the Digital Services Act);

8) “online interface” corresponds to the term used in Article 3(m) of the Digital Services Act.

[*10 November 2005; 19 May 2011; 23 November 2020; 27 April 2023; 23 May 2024*]

**Section 2. Purpose and Scope of Application of the Law**

(1) The purpose of the Law is:

1) to ensure free circulation of information society services in the countries of the European Economic Area (hereinafter also – the country);

2) to ensure transparency of the terms and conditions of a contractual relationship offered by the providers of online intermediation platform services;

3) to ensure the protection of hosting service providers against their misuse for the dissemination to the public of terrorist content online;

4) to facilitate safe, predictable, and trusted online environment.

(2) This Law applies to the provision of information society services, except for the areas regulated by laws and regulations regarding:

1) lotteries and gambling in which a monetary prize is provided;

2) the protection of personal data.

[*23 November 2020; 27 April 2023; 23 May 2024*]

**Section 3. Freedom to Provide Information Society Services**

A service provider which is registered in any of the European Economic Area countries and meets the requirements of the legal acts of the co-ordinated field of the relevant country is entitled to exercise the freedom to provide information society services in the co-ordinated field in Latvia.

**Chapter II. Provision and Storage of Information**

[*19 May 2011*]

**Section 4. Information to be Provided Generally**

(1) A service provider shall provide the following information in a clear, direct, and permanently accessible manner:

1) the firm name (name) or given name and surname, legal address or declared place of residence and registration number (if any) of the service provider;

2) the contact information of the service provider, including electronic mail address, which ensures the possibility to communicate quickly and in a direct manner;

3) if a special permit (licence) is necessary for performing the relevant activity, information on the institution which has issued the special permit (licence);

4) in relation to a regulated profession, information on the professional organisation which has issued the documents confirming the professional qualification, the name corresponding to the profession or qualification, and the country in which it has been granted, and also a reference to the professional regulations applicable in the registration country and the way in which they may be accessed;

5) if the relevant activity is taxable with value added tax, the registration number in the State Revenue Service Value Added Tax Taxable Persons Register.

(2) If a price is indicated, the service provider shall indicate it so that the price is unambiguous and clearly legible and shall provide information on whether or not the taxes to be paid and product delivery costs are included in the price.

[*19 May 2011*]

**Section 5. Information to Be Provided Prior to the Placing of an Order**

(1) A service provider has the obligation to ensure that at least the following information is available to a service recipient before the placing of an order:

1) the procedures which must be complied with to place an order;

2) the conditions for the storage of the signed contract (whether the signed contract is stored) and the availability thereof to the service recipient;

3) the technical means for the detection and correction of input errors prior to the placing of an order;

4) languages offered for entry into the contract.

(2) If the service recipient is not a consumer, the parties may agree upon other procedures for the provision and receipt of information which differ from the procedures provided for in Paragraph one of this Section.

(3) The provisions of Paragraph one of this Section do not apply to the orders which are placed via electronic mail or any other electronic communications means.

**Section 6. Placing an Order**

(1) If a service recipient places an order, the service provider shall acknowledge the acceptance thereof by electronic communications means.

(11) An order and the acknowledgment of the acceptance thereof shall be deemed to be received when the parties to whom they are addressed are able to access them.

(2) A service provider has the obligation to ensure service recipients with the possibility to detect and correct information input errors prior to the placing of an order.

(3) The requirements specified in Paragraph two of this Section need not be applied if the service recipient is not a consumer.

(4) The provisions of Paragraphs one and two of this Section do not apply to the orders placed via electronic mail or equivalent individual means of communication.

[*19 May 2011*]

**Section 7. Information on Terms and Conditions of a Contract and the Codes of Conduct**

(1) A service provider has the obligation to ensure that service recipients may become acquainted with the terms and conditions of a contract and also save them.

(2) A service provider has the obligation to provide information on the codes of good service provision practice or any other voluntary codes of conduct or ethics which they comply with and the information on how to become acquainted with these codes in electronic form.

(3) The requirements specified in Paragraph two of this Section need not be applied if the service recipient is not a consumer.

**Section 7.1 Storage of Information in Terminal Equipment**

(1) Storage of information in a terminal equipment of a subscriber or user or acquisition of access to the information stored in a terminal equipment shall be permitted if the relevant subscriber or user has provided his or her consent after he or she has received clear and comprehensive information on the purpose of the abovementioned processing in accordance with the Personal Data Protection Law.

(2) The consent referred to in Paragraph one of this Section shall not be necessary if the storage of information in a terminal equipment or acquisition of access to the information stored in a terminal equipment is necessary for ensuring circulation of information in the electronic communications network or for the intermediary service provider in order to provide a service requested by a subscriber or user.

[*19 May 2011; 23 May 2024*]

**Chapter III. Commercial Communications**

**Section 8. Information on Commercial Communications**

(1) A commercial communication shall conform to the general requirements of the Advertising Law and also the following requirements:

1) it is clearly recognisable as a commercial communication;

2) the person on behalf of whom this commercial communication is distributed is clearly identifiable;

3) the content of the offer and the conditions for receiving the service are precisely formulated;

4) discounts, bonuses, and prizes are clearly recognisable, and the requirements for the receipt thereof are clearly set out;

5) advertising competitions, lotteries or games are clearly identifiable and the relevant terms of participation are easily accessible as well as explicitly outlined;

6) the service recipient is given the possibility to refuse to receive further commercial communications.

(2) If a person exercising a regulated profession provides a commercial communication with regard to an information society service, this person has the obligation to comply with the professional regulations, especially with regard to independence, respect and professional honour, professional secrets and fairness towards clients and other representatives of the profession.

**Section 9. Prohibition to Send a Commercial Communication**

(1) It is prohibited to use automated calling systems (terminal equipment) without human intervention (automatic calling machines), electronic mail or facsimile machines (fax) for sending a commercial communication by using which an individual contact is possible with a service recipient if the service recipient has not given prior free and explicit consent.

(2) A service provider who, within the framework of their commercial transactions, has acquired electronic mail addresses from service recipients may use them for other commercial communications provided that:

1) commercial communications are sent for similar products or services of the service provider;

2) a service recipient has not initially objected to the further use of the electronic mail address;

3) a service recipient is explicitly given free of charge opportunity to refuse from the further use of electronic mail address on the occasion of each further receipt of a commercial communication (by submitting a submission or sending a electronically).

(3) Communication of other type by using publicly available electronic communications services for sending a commercial communication may occur if the service recipient has given prior free and explicit consent, except for the cases referred to in Paragraphs one and two of this Section.

(4) It is prohibited to use electronic mail or communication of other type by using publicly available electronic communications services for sending a commercial communication if an invalid electronic mail address, invalid phone or fax number is used to which the service recipient might send a request to cease such communication or if the refusal of the service recipient from further receipt of commercial communications is not taken into account.

(5) Sending of each prohibited commercial communication is a separate breach.

(6) The prohibitions and restrictions specified in Paragraphs one, two, and three of this Section do apply to the sending of commercial communications to natural persons.

[*10 November 2005; 12 June 2009*]

**Chapter IV. Liability and Obligations of an Intermediary Service Provider**

[23 May 2024]

**Section 10. Liability of an Intermediary Service Provider**

[23 May 2024]

**Section 11. Obligations of an Intermediary Service Provider**

[23 May 2024]

**Chapter IV.1 Representation of the Interests of Business Users or Corporate Website Users**

[*23 May 2024*]

**Section 11.1 Rights and Obligations of Associations and Foundations**

(1) In order to represent business users or corporate website users in legal proceedings, an association or a foundation which conforms to the requirements of Article 14(3) of Regulation No 2019/1150 has the right to submit to the Consumer Rights Protection Centre the request to grant the right to the association or foundation to represent business users or corporate website users before a court.

(2) If changes have been made to the activities of an association or a foundation due to which the association or foundation does not conform or might not conform to the requirements of Article 14(3) of Regulation No 2019/1150 or if the association or foundation wishes to withdraw its request to represent business users or corporate website users in legal proceedings, the foundation or association has the obligation to immediately inform the Consumer Rights Protection Centre thereof.

(3) The association or foundation shall submit the documents referred to in Paragraphs one and two of this Section which have been signed in accordance with the procedures laid down in the laws and regulations regarding electronic documents to the Consumer Rights Protection Centre electronically.

[*23 May 2024*]

**Section 11.2 Obligations of the Consumer Rights Protection Centre**

(1) The Consumer Rights Protection Centre shall examine the documents referred to in Section 11.1, Paragraphs one and two of this Law and inform the association or foundation of one of the following decisions taken:

1) to grant the association or foundation the right to represent business users or corporate website users before a court;

2) to refuse to grant the association or foundation the right to represent business users or corporate website users before a court;

3) to terminate the right of the association or foundation to represent business users or corporate website users before court.

(2) The Consumer Rights Protection Centre shall inform the European Commission of the decision taken in Paragraph one, Clauses 1 and 3 of this Section.

(3) The decisions referred to in Paragraph one of this Section may be appealed to the District Administrative Court in accordance with the procedures laid down in the Administrative Procedure Law.

[*23 May 2024*]

**Chapter V. Supervision of the Circulation of Information Society Services**

**Section 12. Supervisory Bodies**

(1) The Consumer Rights Protection Centre, State Data Inspectorate and also other supervisory and control bodies shall, within the limits of their competence, supervise the circulation of information society services.

(2) Supervisory bodies shall provide service providers and service recipients with information on the procedures for the examination of complaints and other information.

[*10 November 2005*]

**Section 13. Rights and Obligations of Supervisory Bodies**

(1) If a supervisory body establishes violations of this Law, it is entitled to:

1) request all the information necessary for the clarification of the substance of a case;

2) order the service provider to stop the violation of the Law or to perform particular activities for the elimination thereof, and also to specify the time limit for the performance of these activities.

(2) The supervisory body is entitled to perform the activities specified in Paragraph one of this Section which restrict the provision of such an information society service which creates or may create serious risk, provided that these activities are proportional to the protection of the relevant interests and are necessary for:

1) the interests of the public, especially for the prevention and investigation of criminal offences and the initiation of a case, including for the protection of minors in order to prevent the discrimination of a person based on his or her race, sex, religious convictions or ethnic origin, and also violations injuring the dignity and honour of a person;

2) public safety, including national security and defence;

3) public health protection;

4) consumer protection.

(3) Prior to performing the activities referred to in Paragraph two of this Section, a supervisory body shall inform the State supervisory body in which the relevant service provider is registered and request that it take actions in order to stop the violation referred to in Paragraph two of this Section. The supervisory bodies of Latvia shall inform the European Commission and the relevant country of the activities they are planning to perform if these countries do not perform activities for the elimination of the violation or the activities performed thereby are not sufficient.

(4) In urgent cases when there is a justified reason to deem that public safety, health or consumer interests will be endangered, a supervisory body may perform the activities referred to in Paragraph two of this Section prior to informing the European Commission and the relevant country. In such case, the supervisory body shall immediately inform the European Commission and the relevant country of the activities performed and justify the urgency of these activities.

(5) The Cabinet shall determine the responsible body which coordinates the circulation of the information referred to in Paragraphs three and four of this Section between the supervisory bodies of Latvia, the supervisory bodies of the European Economic Area countries and the European Commission.

(6) A supervisory body has the obligation to inspect compliance with Section 9 of this Law if one service recipient has received at least 10 commercial communications from one service provider during one year and if the service recipient has submitted a complaint to a supervisory body thereon.

[*10 November 2005; 12 June 2009*]

**Chapter VI. Supervision of the Providers of Online Intermediation Platform Services**

[*23 November 2020*]

**Section 14. Supervisory Body of the Providers of Online Intermediation Platform Services**

(1) Providers of online intermediation platform services shall be supervised by the Consumer Rights Protection Centre within the limits of its competence.

(2) The Consumer Rights Protection Centre shall supervise the fulfilment of the transparency provisions of online intermediation platform services by evaluating the influence of the possible violation on commercial users or corporate website users, and also shall ensure that the providers of online intermediation platform services comply with the requirements of Regulation No 2019/1150. The Consumer Rights Protection Centre shall carry out the supervision:

1) upon its own initiative;

2) on the basis of the submission of a business user or corporate website user or the collective submission of the abovementioned users;

3) on the basis of the submission which has been submitted by an association or foundation within the meaning of Article 14(6) of Regulation No 2019/1150.

[*23 November 2020*]

**Section 15. Rights and Obligations of the Consumer Rights Protection Centre**

(1) The Consumer Rights Protection Centre has the right to take one or several decisions referred to in this Paragraph:

1) to request and receive from providers of online intermediation platform services, business users or corporate website users all the information necessary for the supervision thereof and other proof, and also verbal explanations on the conformity of the activities of the providers of online intermediation platform services with the requirements of Regulation No 2019/1150 and determine the time limit for the provision of the abovementioned information and proof and the type of provision of the information;

2) to impose an obligation on the providers of online intermediation platform services to prevent the violation of Regulation No 2019/1150 and also to determine the time limit for the performance of the relevant activities;

3) in accordance with Section 16 of this Law, to impose a fine if the Consumer Rights Protection Centre has recognised the activities of the providers of online intermediation platform services to be non-conforming to the requirements of Regulation No 2019/1150.

(2) The Consumer Rights Protection Centre shall take the decision on the violation of Regulation No 2019/1150 within six months from the day of initiation of the case. If this term cannot be complied with due to objective reasons, the Consumer Rights Protection Centre may extend it for a period which does not exceed two years by counting from the day of the initiation of the case.

[*23 November 2020*]

**Section 16. Imposition of a Fine and Provisions for the Forced Enforcement**

(1) The Consumer Rights Protection Centre is entitled to impose a fine of up to EUR 14 000 on a provider of online intermediation platform services for the violation of Regulation No. 2019/1150.

(2) When taking the decision on the imposition of a fine and the amount thereof, the Consumer Rights Protection Centre shall evaluate and take into account the following circumstances:

1) the nature and duration of the violation admitted, impact caused by the violation (losses for a business user or corporate website user), circumstances of the commitment of the violation, the role of the violator in the violation, and the scope of the violation;

2) whether the provider of online intermediation platform service has compensated or started to compensate the losses caused to a business user or corporate website user by the day of taking the decision;

3) whether the violation is interrupted upon initiative of the provider of online intermediation platform services;

4) whether the provider of online intermediation platform services has committed a repeated violation of Regulation No 2019/1150 within the last two years and whether it has been established by the decision of the Consumer Rights Protection Centre;

5) whether the provider of online intermediation platform services has delayed examination of the case or concealed the violation committed.

(3) The provider of online intermediation platform services shall pay the fine imposed by the Consumer Rights Protection Centre within a month from the day when the decision on the impositions thereof has come into effect.

(4) If the decisions which are taken in accordance with Section 15, Paragraph one, Clause 2 of this Law have not been complied with voluntarily, the Consumer Rights Protection Centre may, when performing the forced enforcement of the decision addressed towards a certain activity, impose a pecuniary penalty, but not more than EUR 2800 at one time.

(5) When determining the amount of a pecuniary penalty referred to in Paragraph four of this Section, the Consumer Rights Protection Centre shall take into account the impact of non-compliance with the decisions referred to in Section 15, Paragraph one, Clause 2 of this Law (losses for a business user or corporate website user) and the duration thereof, and also other circumstances which are relevant to the case.

(6) The paid fine or pecuniary penalty shall be transferred into the State basic budget.

[*23 November 2020*]

**Section 17. Appealing the Decision of the Consumer Rights Protection Centre**

The decision of the Consumer Rights Protection Centre may be appealed to a court in accordance with the procedures laid down in the Administrative Procedure Law. Appealing the decision of the Consumer Rights Protection Centre shall not suspend the operation thereof, except for the operation of the decision referred to in Section 15, Paragraph one, Clause 3 of this Law.

[*23 November 2020*]

**Chapter VII Supervision of the Prevention of the Dissemination of Terrorist Content**

[*27 April 2023*]

**Section 18. Competence of Institutions**

(1) The State Security Service shall be the competent institution in implementing the measures included in Article 6(2), Article 11(3), Article 12(1)(a), (b), (c), and Article 14(6) of Regulation No 2021/784, i.e. issuing and scrutinising removal orders, overseeing the implementation of specific measures, providing guidance on non-disclosure and storage periods of information removed, communicating with Europol, in particular before issuing removal orders, in order to avoid overlaps with other Member States bound by Regulation No 2021/784.

(2) In compliance with Article 12(2) of Regulation No 2021/784, information on the contact point shall be available on the website of the State Security Service.

(3) A hosting service provider shall inform the contact point of the State Security Service of its appointed legal representative in compliance with Article 17(4) of Regulation No 2021/784.

(4) The State Security Service shall, in cooperation with the State Police, prepare and publish the report provided for in Article 8(1) of Regulation No 2021/784 and collect and send to the European Commission the information referred to in Articles 21(1), 22, and 23 of Regulation No 2021/784, if necessary, by requesting hosting service providers to send the transparency reports referred to in Article 7 of Regulation No 2021/784.

(5) A hosting service provider who needs to inform the contact point in the Republic of Latvia in compliance with Article 14(5) of Regulation No 2021/784 may send the relevant information to Europol through the State Security Service. The contact details of the State Security Service shall be available on its website.

(6) Before issuing a removal order, the State Security Service has the right to send an alert referral to a provider of hosting services about information that could be considered terrorist content in order for it to assess the compliance of the content with its commercial rules within a time limit specified in the alert referral.

(7) The State Security Service has the right to request and a hosting service provider has the obligation to provide the necessary additional information to verify the circumstances specified in Article 18(1) of Regulation No 2021/784 in relation to the established potential infringement.

(8) The State Security Service has the right to impose on a hosting service provider the obligation to remedy non-compliance with the requirements of Regulation No 2021/784 within a specified time limit.

[*27 April 2023*]

**Section 19. Legal Remedies**

(1) A removal order issued or a decision taken by the State Security Service may be contested and appealed in accordance with the procedures laid down in the Administrative Procedure Law. The contesting and appeal of a removal order or a decision shall not suspend its operation, nor shall its operation be suspended upon request of a person.

(2) The removed information or content to which access has been disabled shall be stored for the time limit specified in Article 6(2) of Regulation No 2021/784, unless otherwise specified by the institution (authority) responsible for handling the contestation or appeal.

[*27 April 2023*]

**Chapter VII.1 Application of the Digital Services Act**

[*23 May 2024*]

**Section 19.1 Competent Authority and Digital Services Coordinator of the Digital Services Act**

(1) The Consumer Rights Protection Centre shall be the competent authority within the meaning of Article 49(1) of the Digital Services Act and the digital services coordinator within the meaning of Article 49(2) of the Digital Services Act.

(2) The independence requirements laid down in Article 50 of the Digital Services Act shall apply to the digital services coordinator. The digital services coordinator shall take decisions independently and perform the tasks specified in this Law and shall be independent in its activity insofar as it is related to the application of the Digital Services Act.

(3) The digital services coordinator shall be funded in a way to ensure independence of its functions and efficient application of the Digital Services Act in accordance with Section 50 of this Law.

*[23 May 2024]*

**Section 19.2 Obligations, Tasks, and Mutual Cooperation of Institutions**

(1) The Consumer Rights Protection Centre shall perform all tasks of the digital services coordinator specified in the Digital Services Act, including shall supervise the conformity of the activity of intermediary service providers with the obligations specified in Chapter III, Sections 1, 2, 3, and 4 of the Digital Services Act if the European Commission has not commenced a procedure for the same violation in relation to the provider of a very large online platform or very large online search engine within the meaning of Article 33 of the Digital Services Act.

(2) Upon request of the digital services coordinator, other institutions the functions of which include supervision or other activities in matters concerning the Digital Services Act shall provide an opinion to the digital services coordinator within one month from the day of receipt of the request. Institutions may agree on a longer time limit for the submission of the opinion.

(3) The Cabinet shall determine the following:

1) the information to be indicated in the decision referred to in Article 9 of the Digital Services Act in addition to the requirements laid down in Article 9 of this Act and in other laws;

2) the procedures by which annex shall be appended to the decision referred to in Article 9 of the Digital Services Act if the decision applies to restriction of several online resources;

3) the time limits for the enforcement and operation of the decision referred to in Article 9 of the Digital Services Act;

4) the conditions and procedures for the insertion of the information included in the decision referred to in Article 9 of the Digital Services Act or its annex in the machine readable list maintained by the institution;

5) the procedures by which the decision referred to in Article 9 of the Digital Services Act or the request for information referred to in Article 10 of this Act or the information on its enforcement and also other documents shall be notified to the digital services coordinator.

[*23 May 2024*]

**Section 19.3 Rights of the Digital Services Coordinator**

(1) The digital services coordinator has the right to perform inspections in accordance with Article 51(1)(b) of the Digital Services Act without the permission of a court.

(2) When investigating the conformity of the activity of intermediary service providers with the requirements of the Digital Services Act, the digital services coordinator has the right to request and receive the data referred to in Section 105 of the Electronic Communications Law from an electronic communications merchant.

[*23 May 2024*]

**Section 19.4 Elimination and Termination of Violations of the Digital Services Act**

(1) When assessing the established violation of the Digital Services Act in accordance with Article 51(5) of this Act, the digital services coordinator is entitled:

1) to propose that the intermediary service provider ensures the conformity of its activity with the requirements of the Digital Services Act within the time limit stipulated by the digital services coordinator;

2) to propose that the intermediary service provider undertakes in writing to eliminate the established violation in accordance with the requirements of Section 19.5 of this Law within the time limit stipulated by the digital services coordinator;

3) to take the decision to terminate the administrative case by inviting the intermediary service provider to ensure the conformity with the requirements of the Digital Services Act in its subsequent activities.

(2) The intermediary service provider shall, without delay but not later than within three working days after expiry of the time limit specified in the proposal referred to in Paragraph one, Clause 1 of this Section, inform the digital services coordinator of the execution of the proposal, appending evidence attesting thereto. If the conformity of the activity of the intermediary service provider with the requirements of the laws and regulations is not ensured within the specified time limit, the digital services coordinator is entitled to take one or several decisions referred to in Paragraph three of this Section.

(3) If a violation of the Digital Services Act is established, the digital services coordinator is entitled to take one or several decisions by which:

1) the intermediary service provider is imposed with the obligation to terminate the violation without delay or within a specific time limit;

2) a fine and a periodic penalty payment which is specified in Section 19.6, Paragraph one of this Law are applied to the intermediary service provider.

(4) According to the legal address of the digital services coordinator, a judge of a district (city) court shall decide on the authorisation for the digital services coordinator to perform activities on the basis of which the intermediary service provider is assigned the performance of the activities referred to in Article 51(3)(1)(b) of the Digital Services Act whereby access of the recipients of the service of another intermediary service provider to the relevant service of the intermediary service provider or the online application of another intermediary service provider is restricted.

(5) The digital services coordinator shall indicate the following in the submission regarding the authorisation to perform the activities referred to in Paragraph four of this Section:

1) a description of the service which is the subject of the restriction;

2) the means applicable to restriction;

3) the administrative case in which the digital services coordinator will perform these activities and also the period when these activities will be performed;

4) the justification for the necessity of these activities;

5) the reason precluding achievement of the objective of these activities with more commensurate means.

(6) A judge shall, within 72 hours, examine the submission of the digital services coordinator and other documents in which the necessity to perform the activities referred to in Paragraph four of this Section is justified and take the decision to authorise the activities or to refuse the performance of such activities. The decision of the judge shall not be subject to appeal. The decision of the judge shall be sent to the digital services coordinator within 24 hours from the moment of taking the decision.

(7) The judge shall indicate the information referred to in Paragraph five of this Section and the time limit for the execution and duration of the activities referred to in Paragraph four of this Section in the decision to authorise the performance of the abovementioned activities.

(8) The intermediary service provider which is assigned the performance of the activities referred to in Article 51(3)(1)(b) of the Digital Services Act whereby access of the recipients of the service of another intermediary service provider to the relevant service of the intermediary service provider or the online application of another intermediary service provider is restricted shall not be liable for the losses caused to third parties due to the performance of such activities.

[*23 May 2024*]

**Section 19.5 Written Commitment**

(1) A written commitment is a document which is drawn up by the intermediary service provider upon proposal of the digital services coordinator, undertaking to eliminate the violation referred to in the Digital Services Act within a specific time limit. The written commitment may include a commitment of the intermediary service provider:

1) not to perform specific activities;

2) to perform specific activities, including to reimburse the losses caused to the recipients of service of the intermediary service provider or to provide additional information which is necessary to ensure the conformity of the activity of the intermediary service provider with the Digital Services Act.

(2) By signing a written commitment in which the violation and also the type and time limit for the elimination thereof are indicated, the intermediary service provider shall recognise that he or she has committed the established violation. The written commitment shall be deemed received and enter into effect from the moment when the digital services coordinator has approved its acceptance, certifying in writing to the intermediary service provider that the relevant measures are sufficient for the elimination of the violation and its impact. The certification of the digital services coordinator that the written commitment has been accepted shall be notified in accordance with the procedures laid down in the Law on Notification. The time limit for the elimination of the violation shall not exceed the period necessary for the intermediary service provider to take the intended measures and to ensure the conformity with the Digital Services Act, but not longer than three months, except for the cases when the nature of the intended measures justifies a longer time limit.

(3) If the intermediary service provider, in accordance with Section 19.4, Paragraph one, Clause 2 of this Law, commits in writing to eliminate the established violation and the written commitment has entered into effect, the digital services coordinator shall not take the decision referred to in Section 19.4, Paragraph three of this Law and shall terminate the administrative case in the part regarding the violation which the intermediary service provider commits to eliminate. If the digital services coordinator establishes that the written commitment is not being complied with, it is entitled to take the decision referred to in Section 19.4, Paragraph three of this Law.

(4) The intermediary service provider shall, without delay but not later than within three working days after expiry of the time limit specified in Section 19.4, Paragraph one, Clause 2 of this Law, inform the digital services coordinator of the execution of the commitment, appending evidence attesting thereto.

[*23 May 2024*]

**Section 19.6 Imposing of a Fine and Periodic Penalty Payments**

(1) For the violation of the Digital Services Act, the digital services coordinator is entitled to impose a fine on the intermediary service provider in the amount of up to six per cent of the global annual turnover of the intermediary service provider in the previous financial year and, in order to ensure the enforcement of the decision referred to in Section 19.4, Paragraph three, Clause 1 of this Law, a periodic penalty payment up to five per cent for each day from the average daily turnover or global income of the intermediary service provider in the previous financial year which is calculated from the date indicated in the relevant decision.

(2) When investigating the conformity of the activity of the intermediary service provider with the requirements of the Digital Services Act within the limits of its competence, the digital services coordinator is entitled to impose a fine on the intermediary service provider or another person in the amount of up to one per cent of the global annual turnover of the intermediary service provider or person in the previous financial year for the provision of inaccurate, incomplete, or misleading information, for failure to provide a reply or failure to correct inaccurate, incomplete, or misleading information and for failure to comply with the investigation.

(3) The digital services coordinator is entitled to impose for each day a periodic penalty payment on the intermediary service provider or another person in the amount of up to five per cent of the average daily turnover or global income of the intermediary service provider or person in the previous financial year which is calculated from the date indicated in the relevant decision for the failure to fulfil the lawful requirements of the digital services coordinator referred to in Article 51(1) of the Digital Services Act.

[*23 May 2024*]

**Section 19.7 Decision on an Interim Measure**

(1) If the digital services coordinator has a reason to believe that significant harm may be caused to the recipients of service of the intermediary service provider and urgent action is required, the digital services coordinator is entitled, on the basis of a *prima facie* finding, to take the decision referred to in Section 19.4, Paragraph three, Clause 1 of this Law as an interim measure.

(2) The decision on an interim measure shall be in effect from the moment of its notification up to the moment when the decision is revoked or amended by the decision of the digital services coordinator or the final decision of the digital services coordinator enters into effect.

[*23 May 2024*]

**Section 19.8 Appeal of a Decision**

(1) The decision of the digital services coordinator may be appealed to the District Administrative Court in accordance with the procedures laid down in the Administrative Procedure Law. Appeal of the decision shall not suspend the operation thereof, except in the part regarding the imposed fines or periodic penalty payments referred to in Section 19.6.

(2) The decision of the digital services coordinator on an interim measure may be appealed within 10 days from the day of the notification thereof. The appeal of a decision shall not suspend the operation thereof.

(3) The application for the decision of the digital services coordinator on the interim measure shall be examined by a court in the written procedure within 14 days. The decision of the court shall not be subject to appeal and shall enter into effect on the day of the taking thereof.

[*23 May 2024*]

**Chapter VIII Administrative Offences in the Field of Prevention of the Dissemination of Terrorist Content and Competence in Administrative Offence Proceedings**

[*27 April 2023*]

**Section 20. Administrative Offences in the Field of Prevention of the Dissemination of Terrorist Content**

(1) For failure to comply with the obligation laid down in Article 4(7) of Regulation No 2021/784 to reinstate content or access thereto without delay if the content or access thereto can no longer be reinstated afterwards, a warning or a fine of up to three hundred units of fine shall be imposed on the hosting service provider who is a natural person and up to three thousand units of fine on the hosting service provider who is a legal person.

(2) For failure to comply with the obligation laid down in Article 6 of Regulation No 2021/784 to store, for the specified time limit, the removed terrorist content or terrorist content to which access has been disabled or the related data, a warning or a fine of up to four hundred units of fine shall be imposed on the hosting service provider who is a natural person and up to four thousand units of fine on the hosting service provider who is a legal person.

(3) For failure to ensure appropriate technical and organisational safeguards aimed at the protection of removed terrorist content and related data laid down in Article 6 of Regulation No 2021/784, a warning or a fine of up to four hundred units of fine shall be imposed on the hosting service provider who is a natural person and up to four thousand units of fine on the hosting service provider who is a legal person.

(4) For failure to provide, or failure to provide in a timely manner, information on terrorist content related to imminent threat to life laid down in Article 14(5) of Regulation No 2021/784 to the investigating institution or the office of the prosecutor, contact point, or Europol, a warning or a fine of up to four hundred units of fine shall be imposed on the hosting service provider who is a natural person and up to four thousand units of fine on the hosting service provider who is a legal person.

(5) For systematic or persistent failure to remove terrorist content or disable access to it within the time limit specified in all Member States, a fine of up to four per cent of the total turnover of the hosting service provider in the preceding financial year shall be imposed on the hosting service provider.

[*27 April 2023*]

**Section 21. Competence in Administrative Offence Proceedings**

Administrative offence proceedings regarding the offences referred to in Section 20 of this Law shall be conducted by the State Police.

[*27 April 2023*]

**Transitional Provision**

[*23 May 2024*]

The Cabinet shall, by 1 September 2024, issue the regulations referred to in Section 19.2, Paragraph three of this Law.

[*23 May 2024*]

**Informative Reference to European Union Directives**

[*10 November 2005; 19 May 2011*]

The Law contains legal norms arising from:

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’);

2) Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations;

3) 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);

4) 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.

The Law has been adopted by the *Saeima* on 4 November 2004.

President V. Vīķe-Freiberga

Rīga, 17 November 2004