<table>
<thead>
<tr>
<th>QUESTION</th>
<th>ANSWER</th>
<th>SOURCE OF LAW/INFORMATION</th>
<th>ADDITIONAL RELEVANT INFO/DEFINITIONS</th>
<th>COURT RULINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Where is online hate speech established as a criminal offence?</strong></td>
<td>Incitement to hatred is an offense according to the Criminal Code of Czech Republic. The use of online tools to commit an offense based on hatred is considered an aggravating circumstance the Czech criminal code, since the internet platform gives an opportunity to reach out for a larger number of people.</td>
<td>Sections 356, 403, 404 of the Criminal Code[^1] Section 260 of the Law against Support and Dissemination of Movements Oppressing Human Rights and Freedoms[^2] (Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. Available at: <a href="http://files.elsa.org/AA/Final_Report_OHS_Final.pdf">http://files.elsa.org/AA/Final_Report_OHS_Final.pdf</a>, p. 140.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>What is the punishment for online hate speech?</strong></td>
<td>If hate speech is committed via computer systems, then the punishment is imprisonment for six months to three years</td>
<td>Section 356 of the Criminal Code[^1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Is there a law-based obligation for intermediaries to monitor hate speech?</strong></td>
<td>Service providers do not have an obligation to monitor illegal comments.</td>
<td>Section 6 of the Act on Some Information Society Services[^3]</td>
<td>“Service provider” (Service provider of information society services) – means any natural or legal person providing an information society service. ^[^c]</td>
<td></td>
</tr>
<tr>
<td><strong>Who is responsible to remove/block access to hate speech?</strong></td>
<td>Service providers</td>
<td>Section 5 of the Act on Some Information Society Services[^3]</td>
<td>“Service provider” (Service provider of information society services) – means any natural or legal person providing an information society service. ^[^c]</td>
<td></td>
</tr>
<tr>
<td><strong>What is the required time frame,</strong></td>
<td>When the service provider realizes</td>
<td>Act on Some Information Society Services[^3]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[^1]: Sections 356, 403, 404 of the Criminal Code of the Czech Republic.
[^2]: Section 260 of the Law against Support and Dissemination of Movements Oppressing Human Rights and Freedoms.
[^3]: Section 6 and 5 of the Act on Some Information Society Services.
[^c]: Service provider – means any natural or legal person providing an information society service.
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>ANSWER</th>
<th>SOURCE OF LAW</th>
<th>INFORMATION</th>
<th>ADDITIONAL RELEVANT INFO/DEFINITIONS</th>
<th>COURT RULINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>if any, for removing hate speech?</td>
<td>that unlawful content has been posted, it should promptly, &quot;without delay&quot;, take steps to remove or block such content. Otherwise, the operator could be found responsible for the harm caused by hate speech.</td>
<td>Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. Available at <a href="http://files.elsa.org/AA/Final_Report_OHS_Final.pdf">http://files.elsa.org/AA/Final_Report_OHS_Final.pdf</a>, p. 147.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the intermediary liable for hate speech posted on a website?</td>
<td>Yes, under two conditions: 1. If the provider should have known that the content and the user's behavior were unlawful; or 2. If it has been demonstrated to the operator that the nature of the content was irregular or illegal.</td>
<td>Act on Some Information Society Services C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there any online mechanisms for anyone to report about hate speech content?</td>
<td>Yes, a hotline was established by Czech police for users to report online hate speech.</td>
<td>The Czech police hotline is available at <a href="http://www.policie.cz">www.policie.cz</a>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When is the online offence considered to have been committed within the territory/under the country’s jurisdiction?</td>
<td>Czech law applies to service providers who provide their services via a business or branch located in the territory of Czech Republic. Czech law is also applicable on a service provider established in another member state of the European Union which provides services within the Czech Republic.</td>
<td>Section 9 of the Act on Some Information Society Services C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QUESTION</td>
<td>ANSWER</td>
<td>SOURCE OF LAW/INFORMATION</td>
<td>ADDITIONAL RELEVANT INFO/DEFINITIONS</td>
<td>COURT RULINGS</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Are intermediaries/social media sites obligated to disclose the personal data of hate speech offenders?</td>
<td>Under Czech law, social media sites are not obligated to reveal the identity of a person communicating hate speech. However, for the purposes of criminal proceedings, judicial authorities may order telecommunication service providers to disclose this information. Providers of Internet Connection (Service providers) (some telecommunication companies and NOT operators of networking sites) are obligated to reveal users' data (e.g., IP addresses, home address, name) to police in case of an investigation. They are also obligated to store the data for the period of 6 months.</td>
<td>Section 88a Criminal Procedure Code</td>
<td>Act on Electronic Communication (Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. Available at <a href="http://files.elsa.org/AA/Final_Report_OHS_Final.pdf">http://files.elsa.org/AA/Final_Report_OHS_Final.pdf</a>, p. 147.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CZECH REPUBLIC APPENDIX

A. Criminal Code of 2009

Section 356 – Incitement to hatred or restriction of rights and freedoms against a group of persons

“1. Whoever publicly incites hatred against any nation, race, ethnic group, religion, class or other group of persons or to restrict the rights and freedoms of their members shall be punished by imprisonment of up to two years.
2. Whoever conspires to commit an act referred to in paragraph 1 shall be punished in the same manner.
3. The offender shall be punished by imprisonment of six months to three years:
   (a) commits an offense specified in paragraph 1 through the press, film, radio, television, publicly accessible computer networks or other similar effective methods, or
   (b) participating in a group, organization or association that calls for discrimination, violence or racial, ethnic, class, religious or other hatred.”

Section 403 – Foundation, support and promotion of a movement aimed at suppressing human rights and freedoms

“1. Whoever funds, supports or promotes a movement that provably aims at suppressing human rights and freedoms, or spreads racial, ethnical, national, religious or class hatred or hatred against any other group of people, shall be sentenced to a term of imprisonment from one year to five years.
2. An offender shall be sentenced to a term of imprisonment from three to ten years if (a) he/she commits an act as specified in Paragraph (1) via press, motion picture, broadcasting, television, publicly accessible computer network or any other similarly effective way; (b) he/she commits such an act as a member of an organized group; (c) he/she commits such an act as a soldier; or (d) he/she commits such an act during a state of peril to the country or state of war.
3. Preparation is punishable.”

Section 404 – Expressing sympathies for movement aimed at suppressing human rights and freedoms

“Whoever publicly expresses sympathies for a movement as specified in Section 403, Paragraph 1, shall be sentenced to a term of imprisonment from six months to three years.”

B. Law against Support and Dissemination of Movements Oppressing Human Rights and Freedoms of 2001

Section 260

“1. The person who supports or spreads movements oppressing human rights and freedoms or declares national, race, religious or class hatred or hatred against other group of persons will be punished by prison from 1 to 5 years.
2. The person will be imprisoned from 3 to 8 years if:
   (a) he/she commits the crime mentioned in paragraph (1) in print, film, radio, television or other similarly effective manner,
   (b) he/she commits the crime as a member of an organized group
   (c) he/she commits the crime in a state of national emergency or state of war.”

C. Act on Some Information Society Services, 480/2004 Coll.

Section 2 - For the purposes of the present act

27 Available at http://documentostics.com/component/option,com_docman/task,doc_view/gid,1198/.
"a) information society service shall mean any service provided by electronic means at the individual request of a user submitted by electronic means, normally provided for remuneration; a service shall be provided by electronic means if it is sent via an electronic communication network and collected by the user from electronic equipment for the storage of data; b) electronic mail shall mean a text, voice, sound or image message sent over a public electronic communication network which may be stored in the network or in the user’s terminal equipment until it is collected by the user; c) electronic means shall mean in particular an electronic communication network, telecommunications terminal equipment and electronic mail; d) service provider shall mean any natural or legal person providing an information society service; e) user shall mean any natural or legal person who uses an information society service, in particular for the purposes of seeking information or making it accessible; f) commercial communication shall mean any form of communication designed to promote, directly or indirectly, the goods, services or image of an enterprise, a natural or legal person who pursues a regulated activity or is an entrepreneur pursuing an activity that is not a regulated activity; also advertising under a special legal regulation shall be deemed to be commercial communication. Data allowing direct access to the activity of a legal or natural person, in particular a domain name or an electronic-mail address shall not be deemed to be commercial communication; further, data relating to the goods, services or image of a natural or legal person or an enterprise acquired in an independent manner by the user shall not be deemed to be commercial communication; g) automatic, intermediate and transient storage shall mean storage of information provided by the user that takes place for the sole purpose of carrying out the transmission in an electronic communication network, and the information is not stored for any period longer than is usual in order to carry out the transmission; h) automatic, intermediate and temporary storage shall mean storage of information provided by the user that is performed for the sole purpose of making more efficient the information’s onward transmission upon request of other users."

Section 5 - Liability of the service provider for the storage of information provided by a user
"1. A provider of a service that consists of the storage of information provided by a user, shall be responsible for the contents of the information stored at the request of a user only if he
(a) could, with regard to the subject of his activity and the circumstances and nature of the case, know that the contents of the information stored or action of the user are illegal; or
(b) having, in a provable manner, obtained knowledge of illegal nature of the information stored or illegal action of the user, failed to take, without delay, all measures, that could be required, to remove or disable access to such information.

2. A service provider referred to in paragraph 1 shall always be responsible for the contents of the information stored if he exerts, directly or indirectly, decisive influence on the user’s activity."

Section 6 - Extent of the provider’s obligations
"Service providers referred to in Sections 3 to 5 shall not be obliged to
(a) monitor the contents of the information which they transmit or store;
(b) actively seek facts or circumstances indicating to illegal contents of information."

Section 9
"1. Provisions of the present act and of special legal regulations governing the conditions for starting and conduct of an activity which is subject to the service provided, in particular of legal regulations governing the originations of a business license, requirements for professional competence, requirements for contents and quality of the service provided, and liability of the service provider for breach of those obligations shall apply to a service provider who provides services through a business or branch located on the territory of the Czech Republic.

2. Unless provided otherwise in the present act or a special legal regulation, the legal regulations referred to in paragraph 1 shall not apply to a service provider established in - 5 - another member state of the European Union and providing the service on the territory of the Czech Republic.

3. The provisions of paragraph 2 shall be without prejudice to the obligations of a service provider arising out of special legal regulations concerning the protection of public order, public health, state security and consumer protection.

4. Before a court or another authority with the jurisdiction to provide for fulfilment or enforcement of obligations of a service provider arising out of special legal regulations concerning the protection of public order, public health, state security and consumer protection takes the necessary measures, it shall inform the Commission of the European Communities (hereinafter referred to as “Commission”) thereof and request the member state of the European Union in which the service provider is established to take measures resulting in the court no longer having to take measures under the present paragraph.

5. If the court deviates from paragraph 4 in urgent cases, it shall, without unnecessary delay, give the Commission and the member state of the European Union, in which the service provider is established, information and justification thereof."
D. Code of Criminal Procedure

Section 88 - Intercepting and recording the telecommunication operation

"1. If criminal proceedings are conducted for an especially serious intentional crime or for any other intentional crime the prosecution of which is an obligation resulting from a promulgated international treaty, the presiding judge and in pre-trial proceedings the judge based on motion of the public prosecutor may order to intercept and record the telecommunication operation (traffic, transmissions) provided that there is a justified assumption that any fact significant for the criminal proceedings would be communicated through it. It is not allowed to execute any interception or record of telecommunication operation between (defense) counsel and the charged person. If the police body ascertains from the interception and records of the telecommunication operation that the charged person communicates with his/her counsel, the police body is obliged to discontinue the intercepting immediately, destroy the record of the contents, and abstain from using in any way the information it has gained in this connection.

2. An order to intercept and record telecommunication traffic shall be issued in written form and justified. At the same time the period of interception and recording of telecommunication traffic must be stipulated, which cannot be longer than 6 months with possibility of (repeated) prolongation for another 6 months by judge. Judge immediately forwards the copy of an order to a public prosecutor. The Police of the Czech Republic carries out interceptions and recordings of the telecommunication operations (traffic) for the purposes (needs) of all bodies active in (responsible for) the criminal proceedings.

3. Without an order under the subsection 1 of this provision the agency can order an interception and recording of the telecommunication operations or carry out it itself even in the cases not mentioned in the subsection 1, if a user of tapped telecommunication station agrees.

4. If the tapping and registration of telecommunication traffic is to be used as an evidence, it is necessary to attach to it the protocol with the data on the place, time, ways and content of registration, and about the person who made the recording as well. Other records shall be marked and reliably archived; it is necessary to write down in the protocol attached to file where the record is archived. It is possible to use as an evidence the record of telecommunication traffic in another criminal case than in the case in relation to which the record has been made if a prosecution in this another case is conducted also for criminal offence mentioned in subsection 1 of this provision or if user of tapped telecommunication station agrees.

5. If during the interception and recording of telecommunication traffic no facts important for criminal proceedings were find out, it is necessary to destroy the records in prescribed way."

Section 88a

"1. If it is necessary, for the purposes of clarification of the circumstances significant for the criminal proceedings, to identify the data of the telecommunication traffic (transmissions) made, which are subject to the telecommunication secrecy or to which the protection of personal and mediation data applies, the chairman of panel (presiding judge), and the judge in the preparatory proceedings, shall order that the legal entities or natural persons performing the telecommunications services disclose these information to him, or to a public prosecutor or police agency in the preliminary proceedings. The order to identify the data of the telecommunication traffic must be issued in writing including its grounds (justification).

2. No order in accordance with subsection 1 is required if the user of the telecommunication device, which the data of the telecommunication traffic are to apply to, gives the consent to disclose the data."