No. 358/2014

The Permanent Mission of the Czech Republic to the United Nations and other International Organisations in Geneva presents its compliments to the Office of the United Nations High Commissioner for Human Rights and with reference to the letter of 26 February 2014 regarding the protection and promotion of the right to privacy in the digital age has the honour to enclose its response.

The Permanent Mission of the Czech Republic avails itself of this opportunity to renew to the Office of the United Nations High Commissioner for Human Rights the assurances of its highest consideration.

Geneva, 22. 4. 2014

STÁLÁ MISE ČESKÉ REPUBLIKY
1
Ženeva

Enclosure: 3 pages

Office of the United Nations High Commissioner for Human Rights
Palais Wilson
G e n e v a
e-mail: registry@ohchr.org

The right to privacy in the digital age - response to the questionnaire

1) What measures have been taken at national level to ensure respect for and protection of the right to privacy, including in the context of digital communication?

The fundamental right to privacy is established by the **Charter of Fundamental Rights of the Czech Republic** (available in English: http://www.usoud.cz/en/charter-of-fundamental-rights-and-freedoms/).

Article 7 (1): *The inviolability of the person and of her privacy is guaranteed. They may be limited only in cases provided for by law.*

Article 13*: No one may violate the confidentiality of letters or the confidentiality of other papers or records, whether privately kept or sent by post or by some other means, except in the cases and in the manner designated by law. The confidentiality of communications sent by telephone, telegraph, or by other similar devices is guaranteed in the same way.*

As to the **specific regulation** of protection of privacy, in 2000 the Czech Republic enacted Act No. 101/2000 Coll., on the protection of personal data (Data Protection Act; available in English: http://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107).

For the Czech Republic as a member state of the European Union, European legislation plays an important role. With regard to personal data protection these documents are directly or indirectly legally binding:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- 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) – this directive was amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, and also by Directive 2009/136/ECPDF file 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.
- Regulation 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

Additionally, the Czech Republic ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108) in 2001 and in the same year it entered into the force in the Czech Republic.

In 2003, the Czech Republic also ratified Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows (Council of Europe, CETS No. 181) and the Additional Protocol CETS No. 181. At this occasion, the Czech Republic has declared that according to Article 3(2)(c) of the Convention CETS No. 108 it will also apply this Convention to personal data files which are not processed automatically.

2) What measures have been taken to prevent violations of the right to privacy, including by ensuring that relevant national legislation complies with the obligations of Member States under international human rights law?

Violations of the right to privacy are sanctioned both as administrative and criminal offences.

The **administrative offenses** are defined and sanctioned by the Data Protection Act (also available in English: http://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107 in Chapter VIII ADMINISTRATIVE DELICTS).

Serious violations of the right to privacy are as **criminal offences** stipulated and penalized by the Act. No 40/2009 Coll., Penal Code. English translation of the Penal Code is not available on-line, therefore the relevant provisions are provided below:

Section 180

Unauthorized Use of Personal Data

(1) Whoever, even out of negligence, publishes, discloses, makes available, or otherwise processes or appropriates personal data that was collected on another person in connection with the execution of public authority without authorization, and thus causes serious harm to the rights or legitimate interests of the person whom the personal data concerns, shall be punished by a prison sentence of up to three years or punishment by disqualification.

(2) Whoever, even out of negligence, violates the State imposed or recognized obligation of confidentiality by publishing, disclosing, making available, or otherwise processing or appropriating personal data that was collected on another person in connection with the execution of their employment, profession, or function without authorization, and thus causes serious harm to the rights or legitimate interests of the person whom the personal data concerns, shall be similarly punished.

(3) An offender shall be punished by a prison sentence of one to five years, monetary penalty, or punishment by disqualification, if,

a) they committed an act referred to in Subsection 1 or 2 as a member of an organized group,

b) they committed such act by the press, film, radio, television, publicly accessible computer networks, or other similarly effective means,

c) they caused substantial damage by committing such an act, or

d) they committed such an act with the intention of gaining a substantial benefit for themselves or someone else.

(4) An offender shall be punished by a prison sentence of three to eight years, if,

a) they caused large-scale damage by committing an act referred to in Subsection 1 or 2 , or

b) they committed such an act with the intention to procure another large-scale benefit for themselves or someone else.

Further, those, who *fail to prevent* others form committing the offence under the Section 180 (*Unauthorized Use of Personal Data),* are liable for a criminal offence under Section 367 (*Failure to act to prevent a crime).*

3) What specific measures have been taken to ensure that procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, are coherent with the obligations of Member States under international human rights law?

- - -

4) What measures have been taken to establish and maintain independent, effective domestic oversight mechanism capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data?

As the Data Protection Act is a comprehensive regulation for personal data protection, and among others, it establishes the **Office for Personal Data Protection**, a central supervisory body with its seat in Prague.

The Office supervises observance of the legal obligations in the area of personal data protection in the scope provided by the Data Protection Act and other specialized laws, international treaties and directly applicable law of the European Communities (for details see http://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107, competences mainly in Chapter IV POSITION AND COMPETENCE OF THE OFFICE).

5) Any other information on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data.

- - -