



EU legislative and partner countries' rules: Social networks and Instagram

Czech Republic



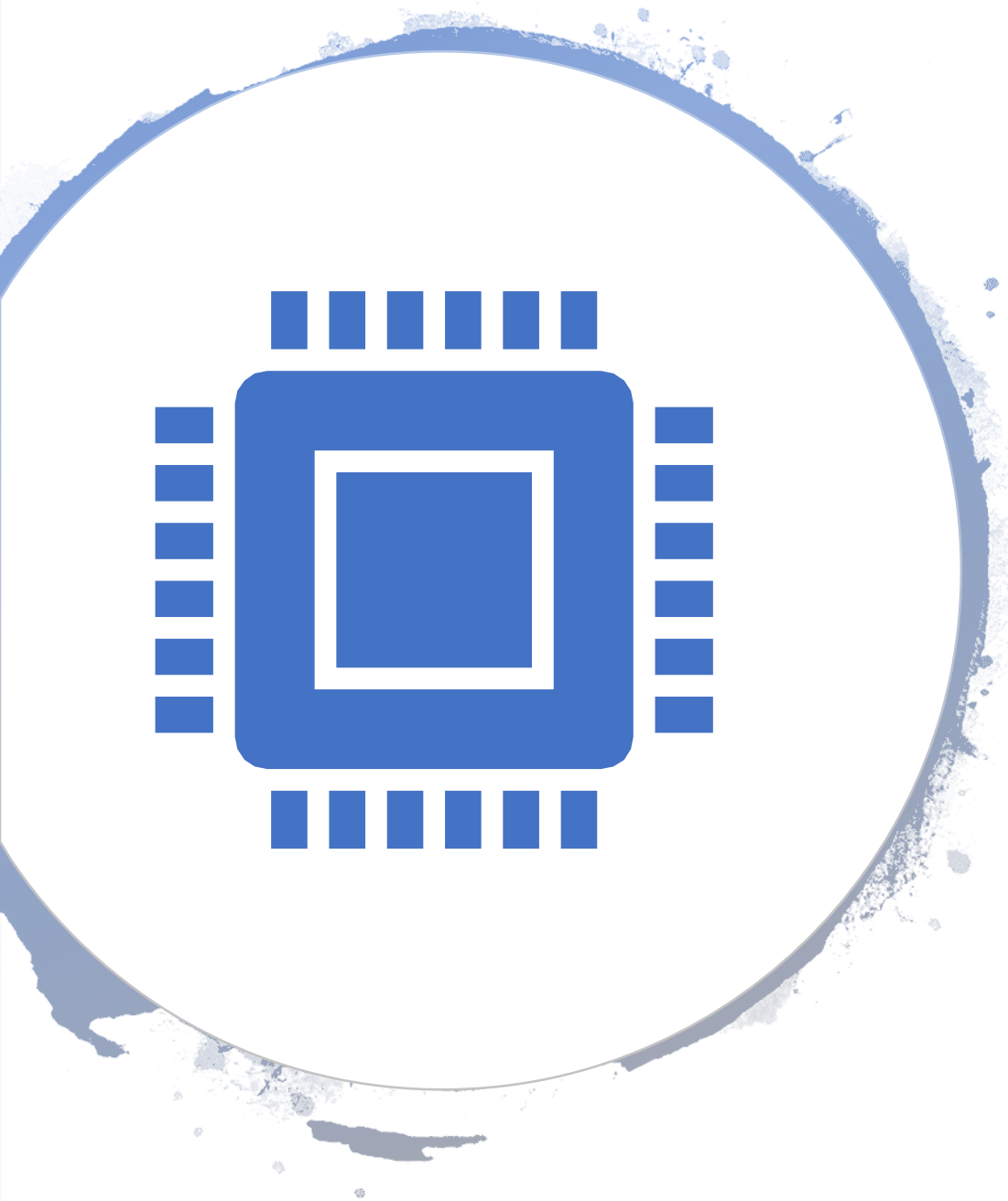
Content

- Cyber Security in the Czech Republic
- Cyber Security Law
- Protection of personal data
- GDPR
- Social networks
- Copyright law
- Copyright law and posting content on Instagram
- Social networks' risks

Cyber Security in the Czech Republic



- The Government of the Czech Republic on 15 March 2010 passed a resolution No. 205 to address cyber security issues and has established the Ministry of Interior of the Czech Republic as a coordinator of cyber security issues and the national authority for the area.



Cyber Security in the Czech Republic

- On 9 December 2010 Ministry of Interior of the Czech Republic with CZ.NIC signed memorandum, and established the National CSIRT.
- Currently, the National CSIRT performs the role of "Point of Contact" for the information technology contributes to the solution of incidents relating to cyber security in the networks operated in the Czech Republic. Until the establishment of government CSIRTs also play the role of "Point of contact" for the network of public and state administration in the Czech Republic.

Cyber Security in the Czech Republic

- On 13 August 2014 president of the Czech republic signed Cyber Security Law (181/ 2014 Coll.) of the Czech Republic. The law is effective since 1st January 2015.
- According to the Law n. 205/2017, the National Cyber and Information Security Agency (NCISA, in Czech: NÚKIB) was established as a competent national authority for the issues of cyber and information security.

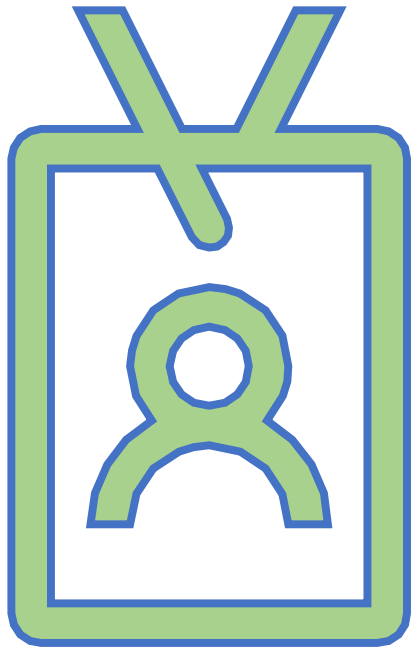




Cyber security Law (181/2014 Coll.)

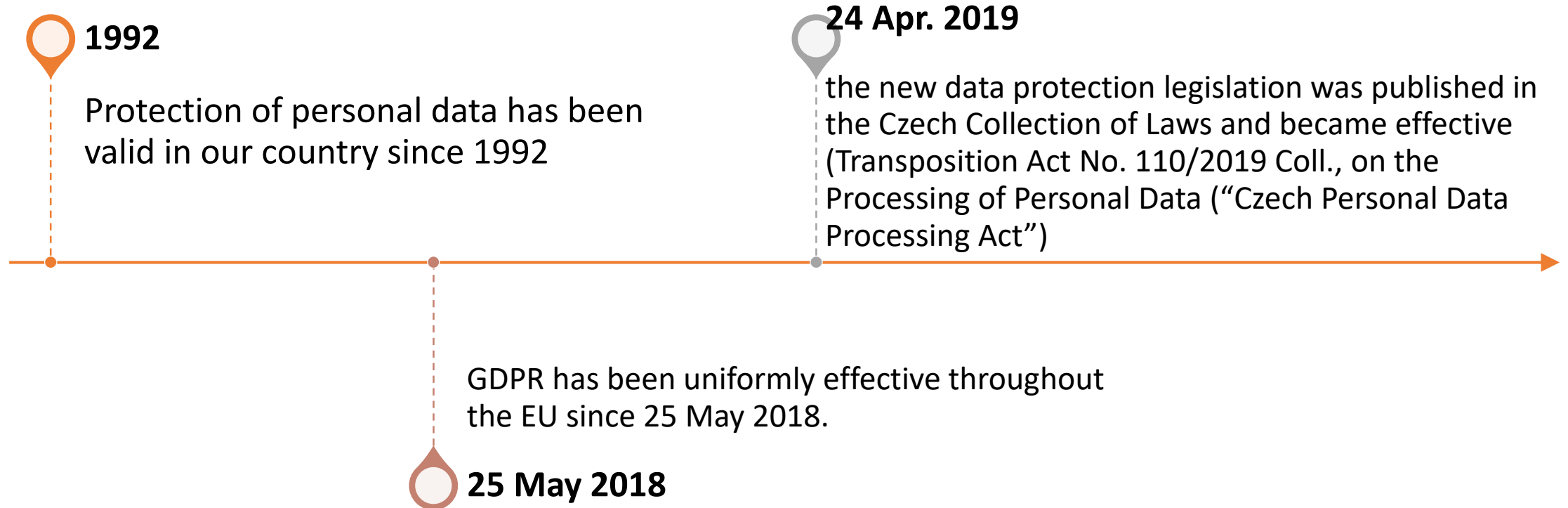
- This Act regulates the rights and obligations of persons and powers of public authorities in the field of cyber security.
- incorporates relevant European Union legislation (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) and regulates the security of electronic communications networks and information systems.

Protection of personal data

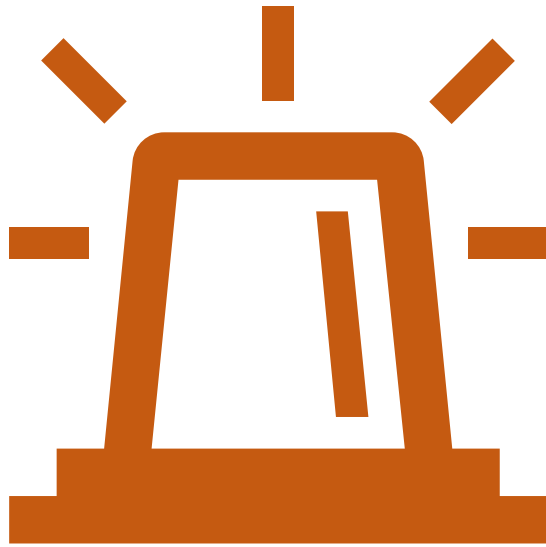


The basis of the right to the protection of personal data (as part of the right to privacy) is, besides European and international law, primarily the constitutional order of the Czech Republic, in particular the Charter of Fundamental Rights and Freedoms to privacy. Article 10 grants contains the right to be protected from the unauthorized collection, disclosure or other misuse of personal data.

GDPR (General data Protection Regulation)



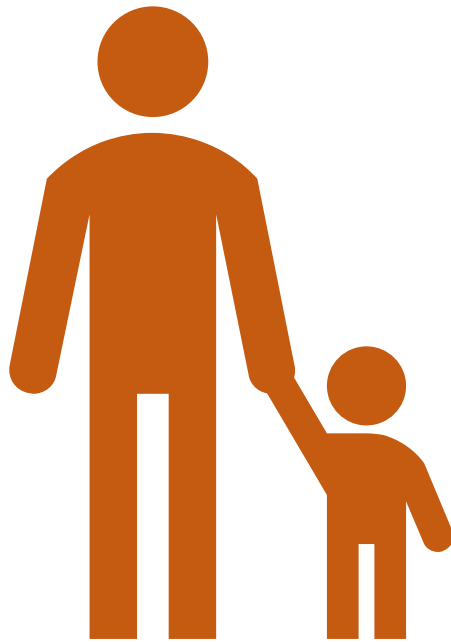
GDPR



Czech Personal Data Processing Act

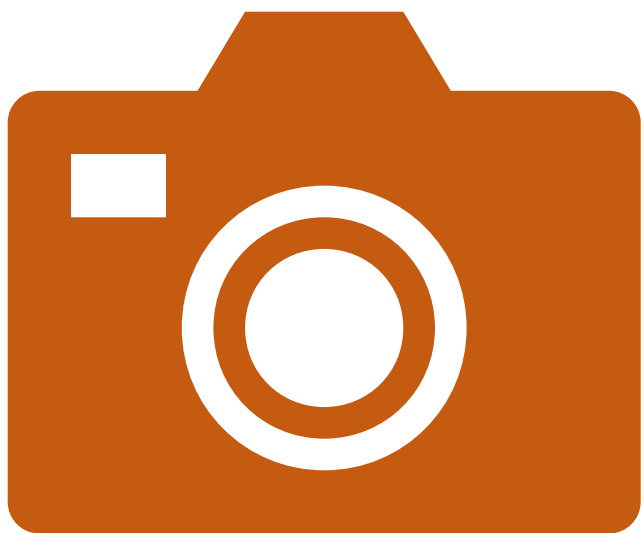
- specifies and further regulates the processing of personal data in accordance with the EU General Data Protection Regulation ("**GDPR**")
- The new Czech Personal Data Processing Act completely abolishes the existing Personal Data Protection Act No. 101/2000 Coll., which remained in effect despite the fact that many of its provisions were in conflict with GDPR

GDPR



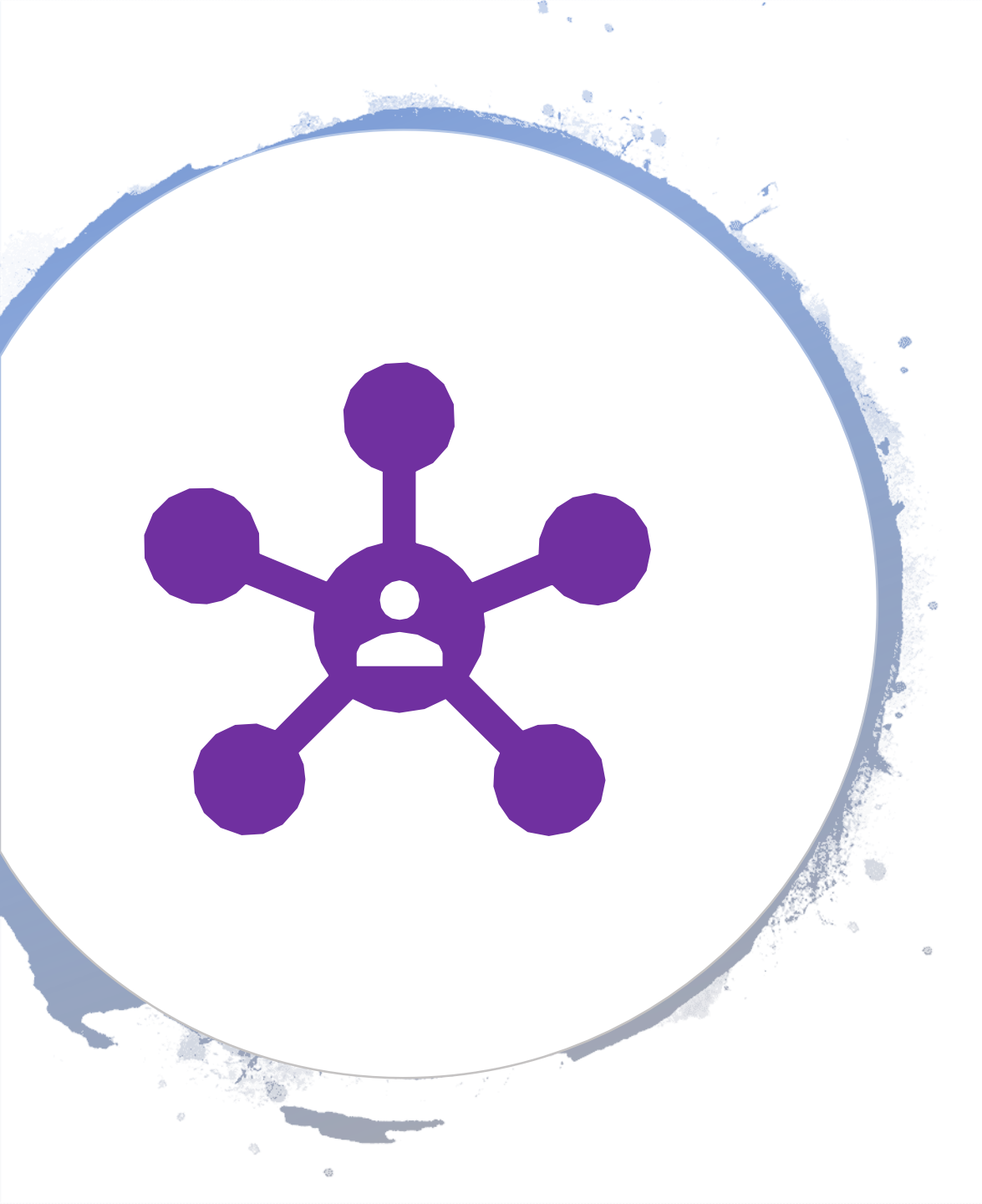
Czech Personal Data Processing Act

- For example, the Act sets a threshold for the eligibility of a child to consent to the processing of personal data in connection with the offer of information society services (e. g. processing of personal data by social network operators) for 15 years. The Czech legislature thus reduced the GDPR threshold by one year.



GDPR – Sharing of photos

- e.g. **holiday photos** - It is simply a personal use that is somehow limited. If someone does not like it, a person has the right under the current law to require you to remove his photo. Or you didn't mention his quote and name.
- **Consent to share photos from the party** - The situation in the workplace is a bit different. For example, your boss needs permission to post a photo of a company party.
- If the photo is used by the employer in the performance of the employee's duties, it may not have the employee's explicit consent
- If a person disagrees with using his / her photo on the Internet, he / she can complain to the Office for Personal Data Protection



Social networks

- Providers use uniform terms and conditions for all their users, regardless of their country of origin.

What is copyright and what does it protect?



- In most countries, copyright is a legal right that protects original copyrighted works. When you create such a work, you usually get the copyright right after you create it.
- Copyright covers all kinds of works, such as:
 - Visual: videos, movies, TV shows and broadcasts, video games, pictures, photos
 - Audio: songs, music tracks, sound recordings, speech recordings
 - Written: books, games, manuscripts, articles, music scores



Copyright law and posting content on Instagram

Before posting content on Instagram, ask yourself the following questions:

- Have I completely created the content myself?
- Do I agree to use all content in my post?
- Is there a copyright exception to the use of the content?
- Is the content protected by copyright (such as a short phrase, idea, or public property)?

Social network risks



The risks are mainly due to the carelessness and imprudence of the users themselves.



Users do not read the terms of use of social services and in this and other ignorance they are not aware that e. g. personal data entered during registration may be easily searched by other users or may be passed on to third parties under the terms of use.



Likewise, sharing information, opinions, photos, etc. - carries its risks if the user profile is not well secured and protected against abuse.



It should be noted that everything that is published on the Internet can usually not be withdrawn. You should think twice about what a user will post about themselves and their privacy.



The risks of social networking primarily related to children can be divided as follows:

- Cyberbullying
- Sexting
- Cybergrooming
- Cyberstalking

social network risks

Identity theft

- Attacks are performed mainly using the phishing technique, where they are lured from the user passwords. Attackers are most interested in the following data:
 - credit card number
 - Credit card security codes
 - passwords - PIN
 - home address
 - date of birth
 - birth number
 - driving license number