## VIII. Safeguards for non-personal data in international contexts

Non-personal data generated by EU companies may be subject to access requests pursuant to provisions of laws of third (non-EU/EEA) countries. This would be specifically relevant when processing of such data occurs in a cloud computing service, the provider of which is subject to the laws of third countries. The recent proposal for a Data Governance Act does not cover such services. The access requests can be of a legitimate nature, in particular for certain cross-border criminal law investigations or in the context of administrative procedures. In particular, these requests may be made in the framework of multilateral or bilateral agreements that determine certain conditions and safeguards. Whereas the GDPR provides for rules and safeguards in this respect, for non-personal data there are currently no statutory law rules that would oblige the cloud computing service providers to give precedence to EU law on the protection of IP and trade secrets. There can be differences in approach between the EU and third countries, e.g. to the fundamental rights safeguards or on the scope of legislation that can mandate access requests to data for law enforcement and other legitimate purposes. Where conflicts of law occur, this may expose the cloud providers to conflicting legal obligations and as a result of this conflict put commercially sensitive data of EU companies at risk.

128. How likely do you think it is that a cloud computing service or other data processing service provider that is processing data on your company's/organisation's behalf may be subject to an order or request based on foreign legislation for the mandatory transfers of your company/organisation data?

- ○ This is a big risk for our company
- ○ This is a risk for our company
- ○ This is a minor risk for our company
- ○ This not a risk at all for our company
- ○ We do not use cloud computing/data processing service provider to store or process our company
- ○ I don't know / no opinion

129. Please explain what order or request for the mandatory transfers of you company/ organization data would you consider as illegitimate or abusive and as such presenting the risk for your company: (200 characters)

CZ would consider as illegitimate or abusive any request for mandatory transfer of data not directly linked to legal or administrative proceedings or unjustified requests presenting trade barriers.

130. Do you consider that such an order or request may lead to the disclosure and/ or misappropriation of a trade secret or other confidential business information?

- ○ This is a big risk for our company
- ○ This is a risk for our company
- ● This is a minor risk for our company
- ○ This not a risk at all for our company
- ○ I don't know / no opinion

131. Does the risk assessment related to such possible transfers of your company /organisation data to foreign authorities affect your decision on selection of the data processing service providers (e.g. cloud computing service providers) that store or process your company/organisation data?

- ● Yes
- ○ No
- ○ I do not use data processing services to store or process my data
- ○ I don't know / no opinion

132. Please explain how it affects your decision (200 characters)

In the Czech Republic, some respondents would favour another provider which can guarantee that client's data would not be shared with the foreign governments.

133. In light of risk assessment of your data processing operations as well as in the context of applicable EU and national legal frameworks (e.g. national requirements to keep certain data in the EU/EEA), do you consider that your company /organisation data should be stored and otherwise processed:

- ○ All of my company/organization data in the EU/EEA only
- ◉ Some of my company/organization data in the EU/EEA only
- ○ All of my company/organization data anywhere in the world
- ○ I don't know / no opinion

134. Please explain what categories of data that should be stored in the EU/EEA only are concerned and why (200 characters)

CZ believes companies should be free to choose where to store/process data but acknowledges the need of critical infrastructure data or data endangering national security to be stored in the EU only.

135. In your opinion, what would be the best solution at an EU regulatory level to mitigate the risk for European companies stemming from the request for access by foreign jurisdiction authorities to their data?

- [x] Introducing an obligation for data processing service providers (e.g. cloud service providers) to notify the business user every time they receive a request for access to their data from foreign jurisdiction authorities, to the extent possible under the foreign law in question
- [ ] Introducing an obligation for data processing service providers to notify to the Commission, for publication on a dedicated EU Transparency Portal, all extraterritorial foreign laws to which they are subject and which enable access to the data they store or process on behalf of their business users
- [ ] Introducing an obligation for data processing service providers to put in place specified legal, technical and organisational measures to prevent the transfer to or access of foreign authorities to the data they store or process on behalf of their business users, where such transfer or access would be in conflict with EU or national laws or applicable international agreements on exchange of data
- [x] Providing for compatible rules at international level for such requests.
- [ ] Other solution
- [ ] There is no action needed to address this
- [ ] I do not know / no opinion

136. Please specify (200 characters)

The CZ believes that notification of the user (it still has to be agreed on whether ex-post or ex-ante) and negotiation of compatible rules at an international level would be the best options offered.