National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Business ID No.: 05800226
Data box ID: zzfnkp3

File ref. No.:
350-647/2025-E

Brno, September 3, 2025

Reference No.:
6159/2025-NÚKIB-E/350

WARNING

The National Cyber and Information Security Agency, registered office: Mučednická 1125/31, 616 00 Brno (hereinafter the "Agency"), pursuant to Section 12(1) of Act No. 181/2014 Coll., on cyber security and on amendments to related acts, as amended (hereinafter the "Cyber Security Act"), issues the following

Warning

of cyber security threat consisting of

1. the transfer of system and user data to the People's Republic of China, to the territories of People's Republic of China´s Special Administrative Regions or to entities based in the territories of the People's Republic of China or its Special Administrative Regions, and
2. the remote administration of technical assets carried out from the territories of the People's Republic of China, People's Republic of China´s Special Administrative Regions or by entities based in the territories of the People's Republic of China or its Special Administrative Regions.

The Agency has evaluated this threat as **High – The threat is likely to very likely**.

Authorities and persons who are obliged to implement security measures pursuant to the Cyber Security Act are obliged to evaluate this threat in the context of risk management pursuant to Section 5(1)(d) of Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, cyber security filing requirements and data disposal (hereinafter the "Cyber Security Decree"), at the level of High – The threat is likely to very likely. If an obliged person uses another method for risk evaluation in accordance with Section 5 of Annex 2 to the Cyber Security Decree, the threat must be assessed at a comparable level as would be the case in the procedure pursuant to Article 5(1)(d) of the Cyber Security Decree.

REASONING

1. Section 11(1) of the Cyber Security Act defines measures (actions taken to protect against or address a cyber security threat or incident), which, pursuant to Section 11(2)(a) of the Cyber Security Act, include, inter alia, warnings. According to Section 12(1) of the Cyber Security Act, the Agency issues a warning if it learns of a cyber security threat.

2. Based on facts established during the exercise of its powers, supplemented by unclassified and classified information obtained from domestic and foreign partners, the Agency concluded that the transfer of system and user data to the People's Republic of China (hereinafter "PRC"), to the territories of PRC´s Special Administrative Regions or to entities based in the territories of the PRC or its Special Administrative Regions, and the remote administration of technical assets carried out from the territories of the PRC, PRC´s Special Administrative Regions or by entities based in the territories of the PRC or its Special Administrative Regions, constitutes a cyber security threat and therefore it issues this warning pursuant to Section 12(1) of the Cyber Security Act.

3. A combination of the following observations and findings led to the issuance of this warning.

4. When assessing whether the transfer of system and user data, or the remote administration of technical assets as described in the operative part of this warning pose a threat to the Czech Republic from the cyber security perspective, it is necessary to examine a number of aspects. These include, among others, the trustworthiness of the legal environment of the PRC and its Special Administrative Regions. The trustworthiness level of countries' legal environments has a direct impact on the trustworthiness of the companies that reside in them and are subject to such legal environments. The legal environment of the PRC has been long monitored and analysed by the Agency, based on which the Agency is aware of certain PRC legal regulations that, in combination with other findings (listed below), pose a threat to the security of the Czech Republic. These legal regulations, among other things, allow significant government interventions in the operations of private companies and provide PRC government authorities with tools to enforce the cooperation of private companies in PRC espionage activities, as highlighted in the Security Information Service's annual report for 2024.

5. For example, they include the National Security Law (国家安全法) of 2015, which imposes a general duty on all Chinese citizens and organisations to provide assistance to state authorities in matters of state security. In addition, the National Intelligence Law (中华人民共和国国家情报法) of 2017 stipulates in Article 7 that every citizen and organisation must support national intelligence activities, provide cooperation and collaboration, and maintain confidentiality regarding classified matters that come to their attention in connection with national intelligence activities. Furthermore, the Counter-Espionage Law (中华人民共和国反间谍法) of 2014 imposes the duty to provide cooperation and information on foreign clients of Chinese companies in case they are suspected of espionage activities by state authorities, and according to Article 6, this law also applies to institutions, organisations and individuals who organise or finance espionage activities against the PRC outside its territory, where a wide range of activities can be defined as espionage by the Chinese authorities, all without the possibility of independent judicial review. State authorities of the PRC can, due to the broad and vague definitions provided in this law (e.g., the definition of national security), require companies to provide almost any information, with the companies having de facto no control over the information they hold. In 2023, an amendment to this law came into effect, which expanded not only the definition of espionage but also the overall scope of the law; as a result,

the law applies to any documents, data, or objects that the Chinese authorities determine are related to national security. Another of these regulations is the Company Law (中华人民共和国公司法 2013修订) of 2013, which allows the Communist Party of China (CPC) to effectively influence the operation of private companies. According to Article 19, a CPC organisation must be established in a company for the purpose of carrying out CPC activities in accordance with its articles of association, and a company must ensure the necessary conditions for these activities. The rules for reporting vulnerabilities in network products (公安部关于印发网络产品安全漏洞管理规定的通知) from 2021 are also problematic, as they require technology manufacturers to report security vulnerabilities to the Chinese Ministry of Industry and IT (hereinafter the "MIIT") within two days of their discovery. The MIIT then reports such findings to the PRC Ministry of State Security and other relevant institutions, and technology manufacturers are prohibited from disclosing or reporting these vulnerabilities to foreign organisations and individuals.

6. All these legal regulations allow increased control by the government authorities of the PRC over the Chinese online environment and (among other things) technology companies. At the same time, the CPC intervenes in all areas of civil society (including non-governmental organizations, state-owned enterprises, private companies, and branches of foreign companies based in the PRC). In addition, the Chinese state can interfere with the operation and structures of many formally private companies through ownership interests (so-called Golden Shares), and state supervision of such companies is further deepened by the activities of CPC organisations, which are compulsorily established in these companies based on the aforementioned Company Law (中华人民共和国公司法 2013修订) of 2013. The findings of the Agency's partners confirm that the CPC influences decision-making processes, for example regarding the appointment of the company employees. At the same time, there is strong pressure for managerial positions in these companies to be filled by members of the CPC.

7. The above-mentioned legal regulations of the PRC, which are considered problematic from the perspective of the security of the Czech Republic, are also applicable to the territories of PRC´s Special Administrative Regions, namely Hong Kong and Macau. These are territories that fall under the sovereignty of the PRC, even though they are not part of mainland China. These territories maintain their economic systems and a high degree of autonomy, but the government of mainland China remains responsible for the defence and foreign policy of these regions. An example of a close connection between the PRC and its Special Administrative Regions is the method of appointing the highest representatives of Hong Kong or Macau, i.e., the chairpersons of the Executive Council, who are elected by the electoral commissions of the regions, but are ultimately appointed to their positions by the central government of China.

8. Directly in the territory of Hong Kong, there are some other legal regulations that can also be considered problematic from the perspective of the security of the Czech Republic, for example, the Basic Law of 1990 (香港基本法), Article 23 of which authorizes the Hong Kong legislative power to adopt its own security laws that would provide protection against various anti-state acts (including treason or subversion), not only in relation to Hong Kong but to the

entire PRC, thereby bringing the power and security interests of the PRC directly into the constitutional system of Hong Kong. Another of these regulations is the Safeguarding National Security Ordinance of 2024 (護國家安全條例), through which the integration of the PRC's national security framework into Hong Kong's legislative framework is sought, as a result of which the term 'state secret' contained in this legal regulation can relate de facto to any act of an economic, social, technological, or scientific nature, even if it was not previously designated as a state secret. It is therefore a very vague and unclear legal framework.

9. From the perspective of the security of the Czech Republic, problematic legal regulations can also be identified in the territory of Macau. These include, for example, the Basic Law of 1993 (中华人民共和国澳门特别行政区基本法), which (as in the case of Hong Kong) authorizes the legislative power of Macau to adopt its own security laws that would provide protection against various anti-state acts (including treason or subversion), not only in relation to Macau but to the entire PRC, thereby bringing the power and security interests of the PRC directly into the constitutional system of Macau. Another of these legal regulations is the Cybersecurity Law of 2019 (網絡安全法), which concerns critical infrastructure and gives the Macau authority abbreviated as CARIC (Cybersecurity Incident Alert and Response Center) the mandate to conduct real-time monitoring of computer data transmitted between critical infrastructure network operators and the internet. There is no supervisory mechanism over CARIC, which opens up significant space for surveillance by Macau authorities.

10. From the above analysis of the legal environment of the PRC and its Special Administrative Regions, it follows that the legal regulations in force in these territories allow government authorities to exert active and effective pressure on private companies or entities, which may be forced to prioritize the interests of the PRC or the regions over the interests of entities whose system and user data are transferred to the above-mentioned territories or whose technical assets are remotely managed from these territories, as stated in the operative part of this warning.

11. The risk associated with data transfer to the PRC or to its Special Administrative Regions is further evidenced by a 2021 study titled 'Government access to data in third countries,' prepared for the European Data Protection Board by researchers from the Centre for IT and IP Law at the Catholic University of Leuven. This study states that PRC laws allow broad access by PRC state authorities to data without sufficient independent oversight. According to the Agency, this approach is in stark contrast to the principles of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), which requires transparency, proportionality, and legal protection of data subjects.

12. The methodological guideline of the European Data Protection Board titled 'Guidelines 02/2024 on Article 48 GDPR' states that most data transfers to the PRC are risky and legally unsustainable without additional measures. The risk associated with data transfer to the PRC is further exacerbated by the Chinese Personal Information Protection Law (中华人民共和国

个人信息保护法) from 2021, which grants the CPC extensive powers in the area of supervision and enforcement of information provision on basis of national security, which, like other terms in the law, is defined vaguely and very broadly.

13. The unclear legal framework, which in practice allows PRC government authorities an unlimited access to all data transferred to the PRC (and by extension also to the territories of its Special Administrative Regions), poses a significant threat to the security of the Czech Republic. This is especially true if the transferred (whether system or user) data concerns systems regulated by the Cyber Security Act. These are backbone systems that ensure the provision of very important services in the Czech Republic. Disruption of the availability, confidentiality, or integrity of these systems, or the data contained therein, could therefore potentially have a significant impact on many people in the territory of the Czech Republic. For the same reason, it is also necessary to proactively address the threat posed by the enabling of remote administration of technical assets of these systems carried out as described in the operative part of this warning.

14. The Agency also issued this warning considering the ever-increasing influence of Chinese state or state-supported companies in the field of European critical infrastructure (e.g., energy, 5G networks, or data flows), which the European Parliament also points out in its resolution of 17 January 2024, on the security and defence implications of China's influence on critical infrastructure in the European Union (2023/2072(INI)). The mentioned resolution states that data transfers specifically to Chinese clouds or data centres, subject to the (above-described, problematic) legislation of the PRC, are incompatible with European principles of privacy protection and security.

15. Chinese investments in Czech and European critical infrastructure, as well as Chinese dominance in strategic supply chains, are explicitly identified as a risk by the Security Strategy of the Czech Republic from 2023. A closer analysis of significant Chinese technology companies reveals the risk of misuse of user data. This data can be used not only for commercial purposes but also, given the legislation of the PRC, for the needs of security forces and the state. The risk of misuse of this data increases with the degree of connection of the company to the PRC.

16. The Security Information Service repeatedly warns in its annual reports about the danger posed by the increasing share of Chinese technologies, especially in elements of critical infrastructure. The Security Information Service has long emphasized that, among other things, the technological dependence of the Czech Republic on the PRC, as an autocratic regime with global ambitions to create an effective counterbalance to the G7 countries, is a situation that requires active response. In its 2024 annual report, the Security Information Service directly states that 'China's efforts for commercial and technological dominance pose a challenge to the protection of Czech companies, their know-how, and supply chains.' The Security Information Service also points out the increasing efforts of actors connected to the PRC to attack significant state institutions and test the resilience of critical infrastructure. Part of the collection of information of interest useful for PRC intelligence services also includes private IT companies. This is also evident from a study analysing thousands of academic publications by Chinese researchers, which focus on the simulation of attacks against power grids in Europe

and the United States of America. It is also known that the PRC has been studying European networks for over twenty years, with an emphasis on their potential vulnerability to cyber or physical attacks.

17. Based on its own findings and conclusions, the Agency repeatedly warns that most states (including the Czech Republic) do not have sufficient capacities to regularly and effectively verify the security of technological products, especially in cases where remote management by the manufacturer is enabled, for example, due to the need to deliver security updates. Mere control of the devices, given their complexity, is insufficient. Therefore, users must also consider non-technical factors of the products, such as trust in the manufacturer and the legal or political environment in which the manufacturer operates. Many cyber security authorities in various states agree that the selection of a supplier cannot be conditioned solely on technical aspects. One of the key factors is trust in the supplier not to misuse its unique position for its own benefit or that of its home state or another actor. After all, the Security Information Service, in its annual report for 2023, notes that due to insufficient capacities, states generally do not have full control over the supply chain and must therefore rely on the trustworthiness of the manufacturer. In such cases (especially for elements of critical infrastructure), it is essential to use only the manufacturers from countries with the same or similar political, legal, or business environment. The importance of such cautious behaviour is then amplified not only by the global trend of moving the operation of software products, including their data, to the cloud environment but also by the ever-worsening global security situation, in which the effort to ensure cyber security is becoming significantly more important.

18. In its 2023 annual report, the Security Information Service also emphasizes that increased attention should be paid especially to highly complex personal devices such as smartphones, watches, electric cars, as well as cloud services. The risk associated with these devices or services does not only lie in the possibility of installing highly sophisticated spyware but also in the collection of data on location, data and voice communication, or even the creation of audiovisual recordings. Such data is stored on servers in the PRC, to which the PRC government has access according to Chinese legal regulations. For the above reasons, users of these devices or services should actively inquire whether the devices or services come from territories whose political regime and legislation increase the possibility of data misuse by state authorities. Based on the analysis conducted above in this warning, it can be concluded that the PRC and its Special Administrative Regions fall into such territories. Considering its previous activities, the Agency further adds that in the above context, other risky products include, for example, inverters in photovoltaic power plants, IP cameras, health technology, or so-called smart meters.

19. The Agency considers the issuance of this warning necessary also in view of some harmful activities that the PRC has carried out against the Czech Republic in the past, as these activities are in stark contrast to the security interests of the Czech Republic. The Security Information Service points out these activities, stating in its 2023 annual report that in the mentioned year, the Czech Republic became the target of Chinese cyber espionage aimed at extracting strategic data. In the same year, the Czech Republic also became a victim of Chinese attacks targeting 'post-pandemic attempts of the Western world' to diversify supply chains, which have a direct

impact on the Czech economy. The realisation of these activities by the PRC against the Czech Republic is evidenced, among other things, by a harmful cyber campaign, for which the group APT31, associated with the Chinese intelligence service of the Ministry of State Security, was publicly attributed by the Czech Government in 2025. This group has been attacking one of the unclassified networks of the Ministry of Foreign Affairs of the Czech Republic since 2022. The conclusions of the analysis carried out by the Agency, Military Intelligence, the Office for Foreign Relations and Information, and the Security Information Service clearly show that the PRC and specifically the group APT31 (also known as Zirconium or Judgment Panda), which is associated with a number of attacks against political and other targets, including in other EU member states or NATO allies, are behind this long-term harmful campaign.

20. The Czech Republic is clearly not the only state against which the PRC carries out these harmful activities. Attribution assigning responsibility for a cyber-attack on a state institution to an actor linked to the PRC has already been made by other European Union member states in the past. These states include, for example, Belgium, whose Ministry of Foreign Affairs publicly stated in 2022 that the groups APT27, APT30, and APT31, which are linked to the PRC government, were behind the attack on the Ministry of the Interior. Similarly, the United Kingdom (then a former EU member state) publicly attributed responsibility for a cyber-attack targeting members of the British Parliament in 2021 to the group APT31 in 2024.

21. According to the conclusions of the 2022 annual report of the Security Information Service, the Russian invasion of Ukraine prompted the PRC to increase its interest in the situation in Europe and intensify its cyber espionage activities in this region. In the Czech Republic, this manifested itself, for example, in the implementation of spear-phishing attacks, which in several cases targeted Czech state institutions. The sophistication of the attacks gradually increased, while the number of targets decreased. In some cases, the attack even targeted specific individuals. The fact that the security threat posed by the PRC to the Czech Republic in this context should not be taken lightly is also evidenced by the words of the PRC's Minister of Foreign Affairs, Wang Yi, who publicly stated that the PRC does not wish for Russia to lose the war in Ukraine.

22. States outside the European Union have also faced cyber-attacks by actors linked to the PRC in the past. In particular, the United States of America has repeatedly published attributions in this context since 2014.

23. The seriousness of this (above-described) harmful behaviour by the PRC is also underscored by the active efforts of individual states to jointly address this threat through cooperation. An example of this effort is the activity of the intelligence alliance known as FVEY ('Five Eyes'), which includes the United Kingdom, the United States of America, Canada, New Zealand, and Australia. This alliance, with the support of Germany, Republic of Korea, and Japan, issued an advisory in 2024 describing the tradecraft (TTPs) of an actor known as APT40, which is linked to the PRC government and whose activities had a negative impact primarily on the territory of Australia. The above clearly demonstrates that the harmful cyber-espionage activities of actors linked to the PRC have a global dimension.

24. It is entirely evident that the Czech Republic is not the only state that identifies the transfer of data to the PRC (and to its Special Administrative Regions) or the remote administration of technical assets from the above-mentioned territories as a threat to national security. Due to the unverifiable handling of data transferred to the PRC (there were also cases of even illegal transfer of the data to the PRC) or due to insufficient protection of the rights of data subjects in the PRC, countries such as Italy, Germany, the Netherlands, and Australia have also taken certain measures. Although the mentioned measures in the above countries concerned only certain products and services of Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., the main reasons for their adoption are fundamentally the same as the reasons on which the Agency bases this warning, aiming to minimize the threat posed by the transfer of data to the PRC and its Special Administrative Regions, or the remote administration of technical assets from these territories.

25. The fact that the transfer of data to the PRC or its Special Administrative Regions, or the enabling of remote administration of technical assets from these territories, poses a security threat to the Czech Republic is also evidenced by the decision of the Czech government, which banned the Chinese company Emposat Co., Ltd. from operating a ground satellite station in Vlkoš in the Hodonín region, precisely due to concerns that the PRC could misuse this satellite station for espionage purposes. This is an objectively assessed and real threat emphasized by the Security Strategy of the Czech Republic from 2023, which states that the PRC conducts cyber espionage and seeks to control global data traffic, using various forms of socio-economic pressure and other hybrid tools.

26. The Agency evaluates the threat level as high, i.e. in accordance with the threat assessment scale contained in Annex 2 to the Cyber Security Decree as likely to very likely. The threat level is primarily due to the combination of the untrustworthy legal environment of the PRC, which has a very real potential to be applied also to the territories of PRC´s Special Administrative Regions, and the proven long-term harmful activities of actors linked to PRC government authorities against the Czech Republic, whose activities are in stark contrast to the security interests of the Czech Republic. It is also impossible to overlook the global power ambitions of the PRC and its geopolitical inclination, which fundamentally diverges from the orientation of the Czech Republic. This is confirmed by the Security Strategy of the Czech Republic from 2023, which identifies the PRC as a fundamental systemic challenge in a global perspective and in its direct actions against democratic countries, including the Czech Republic.

27. The Agency recommends that all natural persons whose data could be the target of foreign intelligence activities (persons of interest, i.e. persons who are, for example, in high political, public or decision-making positions) consider restricting or completely prohibiting the use of the technologies or services through which system and user data could be transferred to the PRC or its Special Administrative Regions, or whose technical assets could be remotely administered from these territories, as described in the operative part of this warning.

28. The Agency also recommends the general public to pay increased attention to the access requirements of the technologies or services they use. Similarly, the general public should be interested in how these technologies or services handle the data provided by users (including

whether and where this data is sent). The Agency generally recommends installing and using only those technologies that the user trusts.

29. Since the Agency's task pursuant to Section 22(j) of the Cyber Security Act is to ensure prevention in the area of cyber security, which also includes providing information on identified threats in the area of cyber security, the Agency proceeded to issue this warning. All the above information demonstrates that – within the scope specified in the operative part of this warning – the transfer of system and user data to the PRC or its Special Administrative Regions, or the enabling of remote administration of technical assets from these territories, constitutes a security threat to the Czech Republic, which cannot be addressed only by the usual preventive activities of the Agency. The Agency´s authority to issue this warning is given by the provision of Section 22(b) of the Cyber Security Act.

30. Finally, the Agency points out that in accordance with Section 4(4) of the Cyber Security Act, the bodies and persons referred to in Section 3(c) to (f) of the Cyber Security Act are obliged to take into account the requirements resulting from security measures when selecting a supplier for their information or communication system and include these requirements in the contract they conclude with the supplier. Taking into account the requirements resulting from the security measures pursuant to the first sentence to the extent necessary to comply with the duties pursuant to the Cyber Security Act cannot be considered an unlawful restriction on competition or an unjustified barrier to competition.

Ing. Lukáš Kintr
Director
National Cyber and Information Security Agency