noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

Gegevensbeschermingsautoriteit (GBA)
Drukpersstraat 35
1000 Brussel, België

Per e-mail: contact@apd-gba.be

Vienna, 16 January 2024

noyb Case-No: **C093-01**

Complainant: [redacted]
Aliexpress account: [redacted]
User number: [redacted]
e-mail address: [redacted]

Represented under Article 80(1) GDPR by: ***noyb* – European Center for Digital Rights**
Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria

Respondent: **Alibaba.com Singapore E-Commerce Private Limited**
51 Bras Basah Road #04-08 Lazada One Singapore, 189554 Singapore

Regarding: The transfer of personal data to the People's Republic of China and the resulting violation of Chapter V of the GDPR due to the lack of an adequate level of data protection in that country.

COMPLAINT

1. REPRESENTATION

1. *noyb* – European Center for Digital Rights is a not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms with its registered office in Goldschlagstraße 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *"noyb")* (**Annex 1**).
2. *noyb* is representing the Complainant under Article 80(1) GDPR (**Annex 2**).

2. FACTS PERTAINING TO THE CASE

2.1. Respondent ("AliExpress Singapore")

3. Alibaba is a multinational "*leading global retail e-commerce platform enabling consumers to buy directly from manufacturers around the world*", according to its website.[1] More specifically, Alibaba provides users with access to an e-commerce platform called AliExpress, on which users can sell ('Seller') or purchase ('Buyer') a variety of goods.[2]
4. Alibaba.com Singapore E-Commerce Private Limited (hereinafter: "*Respondent*" or "*AliExpress Singapore*") is part of the Alibaba International Digital Commerce Group, which is one of the six groups of Alibaba Group Holding Limited (hereinafter: "*Alibaba Group*").[3] To be accessible worldwide and depending on the scope of business activity, Alibaba Group acts via its subsidiaries, such as the Respondent, AliExpress Russia Holding Private Limited (Singapore), AliExpress E-Commerce One Pte. Ltd (Singapore), Hangzhou Alibaba Advertising Co., Ltd. (Hangzhou, China), etcetera.
5. Alibaba's Group main corporate bodies responsible for data protection, namely the Compliance and Risk Management Committee of the Board of Directors, as well as the Comprehensive Risk Management Working Group and President of the Security Department, are all based in China.[4] Hence, the personal data of the Complainant (and other users established in the EEA) is realistically transferred to China to enable the abovementioned corporate bodies to fulfil their task properly,[5] in particular in case of a data breach.[6] Therefore, each subsidiary of Alibaba

[1] https://www.alibabagroup.com/en-US/about-alibaba-businesses-1747705938191581184

[2] *"AliExpress.com ("AliExpress" or, the "Platform") is a business to consumer (or "B2C") platform which connects and facilitates sales and purchases between business sellers (or "Sellers") and consumer buyers (or "Buyers").*" (**Annex 3**, Introduction).

[3] https://www.alibabagroup.com/en-US/about-alibaba-businesses

[4] Alibaba Environmental, Social, and Governance Report. 2024, link, p. 150 and p. 158.

[5] Alibaba Environmental, Social, and Governance Report. 2024, link, p. 150: "*The Compliance and Risk Management Committee of the Board of Directors is under the direct leadership of an independent director working as its Chairperson. It is responsible for overseeing compliance and risk management across the Group.*"

[6] Alibaba Environmental, Social, and Governance Report. 2024, link, p. 162.

Group, including but not limited to the AliExpress Singapore, is realistically obliged to share data with their Chinese headquarter.

6. By offering its Platform to EU/EEA users, AliExpress Singapore is offering goods and services to data subjects in the Union, as described in Article 3(2)(a) GDPR. Therefore, the GDPR is applicable. That AliExpress is in fact explicitly offering its Platform service to data subjects in the Union, is (among other things) confirmed by the fact that its Privacy Policy is clearly directed to EU/EEA users as well.[7]
7. Based on widely available public reporting, the Complainant assumes that the Respondent's main establishment within the EU is located in Belgium. A facility located in the Belgian city of Liège (a subsidiary of Alibaba Group, called Cainiao Smart Logistics Network Limited,[8] also known as AliExpress' European hub or Cainiao Liège eHub[9]) is responsible for managing purchases of European clients of AliExpress Singapore.[10] While there may be other smaller sales offices of Alibaba in Europe, there is no indication of any similar, let alone larger, establishment than the hub in Liège or any decision-making as to the purposes of means of processing in Europe.

2.2. Complainant

8. The Complainant is a user ('Buyer') of the AliExpress' e-commerce platform (hereinafter: "Platform") since [redacted]. To use the Platform and to buy products on the Platform, the Complainant had to create an account and provide personal data to do so. According to the Privacy Policy of the Platform, the Platform collects and processes personal data, such as contact data (name, address, phone number, e-mail address), financial data (payment data), passport or ID card data (used for user verification) and platform usage and social media information (**Annex 3A**, **Annex 3B**, **Annex 3C** Section A).
9. Since the Complainant's habitual residence is located within the EU/EEA, the Complainant's personal data are processed, in particular, by AliExpress' place of its central administration in the Singapore by AliExpress Singapore (**Annex 3A**, **Annex 3B**, **Annex 3C** Introduction).[11]

---

[7] **Annex 3A**, **Annex 3B**, **Annex 3C** e.g. Section J.

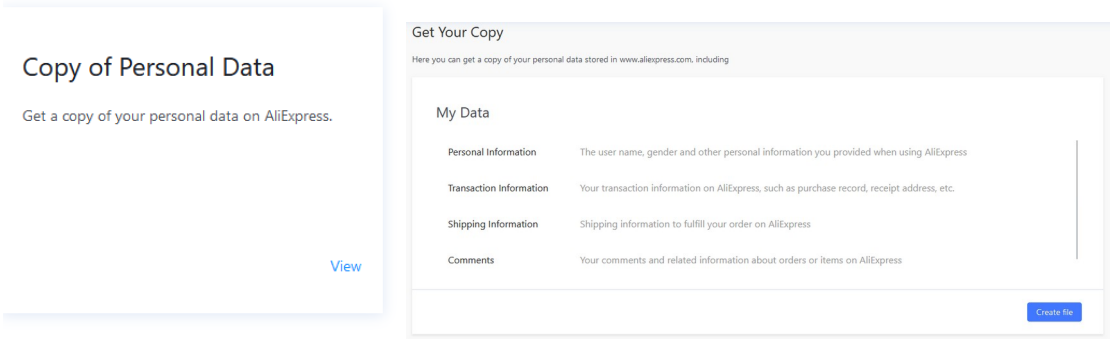
[8] https://www.alibabagroup.com/en-US/about-alibaba-businesses; https://global.cainiao.com/

[9] https://www.linkedin.com/showcase/cainiao-liege-ehub/

[10] https://www.ft.com/content/256ee824-9710-49d2-a8bc-f173e3f74286 ; https://www.reddit.com/r/Aliexpress/comments/lvayiu/why_is_everything_coming_to_europe_being_sent_to/?rdt=49110; https://www.belganewsagency.eu/belgian-intelligence-monitors-alibaba-hub-over-espionage-concerns

[11] "*If you are a registered member of the Platform, and either (a) you are from a place other than mainland China, and United States; or (b) you access and use the Platform from any of the Relevant Jurisdictions, you are contracting with Alibaba.com Singapore E-Commerce Private Limited* […]." (**Annex 3A**, **Annex 3B**, **Annex 3C** Introduction).

10. On [redacted] 2024, the Complainant tried to access her personal data, to verify whether her personal data was being transferred to China or any other third country by AliExpress Singapore. For that purpose, the Privacy Policy (**Annex 3A**, Section O, **Annex 3B**, **Annex 3C** Section P) directed her to the website https://privacy.aliexpress.com/, where she could download a "*Copy of Personal Data*" of her personal data after logging in with her account details (**Screenshot 1-2**).[12] After downloading the files, it turned out that AliExpress Singapore provided the Complainant with a broken file, which could only be opened once.[13]



Screenshot 1-2. The complainant pressed the "View" button under "Get a copy of your personal data on AliExpress", which lead to a webpage where she pressed the "Create File" button to receive a "Copy of Personal data".[14]

11. Since downloading a "*Copy of Personal Data*" did not provide the Complainant with any information under Article 15(1) or (3) GDPR about the data transfers to third countries, data location or any other information about the data processing, she decided to file an access request under Article 15 GDPR on [redacted] 2024 (**Annex 4A**). The access request was sent to DataProtection.AE@aliexpress.com, the e-mail address provided in the Respondent's Privacy Policy (**Annex 3A**, Section O.).
12. The Respondent sent a message "*generated by an auto-reply program*" to this access request of the Complainant on [redacted] 2024 (**Annex 4B**).
13. On [redacted] 2024 the Respondent replied to the access request via email. In this email the Respondent referred the Complainant to the information in its Privacy Policy and to the possibility of downloading a "*Copy of Personal Data*"

[12] https://privacy.aliexpress.com/home#/ which linked to after clicking the "*View*" button under "*Get a copy of your personal data on AliExpress*": https://privacy.aliexpress.com/home#/request/backup where she pressed "*Create File*" to download a "*Copy of Personal Data*".
[13] Therefore, the Complainant is not able to add this file as an annex to this Complaint.
[14] https://privacy.aliexpress.com/home#/ which linked to after clicking the "*View*" button under "*Get a copy of your personal data on AliExpress*": https://privacy.aliexpress.com/home#/request/backup where she pressed "*Create File*" to download a "*Copy of Personal Data*".

(which as is stated above, did not provide the Complainant with a copy of her personal data in practice) (**Annex 4C**).

14. However, none of these responses did include an answer to the Complainant's questions regarding data transfers to China or any other third country by AliExpress Singapore.

2.3. AliExpress' Privacy Policy

15. The Respondent provides a Privacy Policy on its website.[15] When the Complainant sent the access request to the Respondent on [redacted] 2024 (**Annex 4A**), the version of June 21st 2022 was applicable (**Annex 3A**).
16. However, the Respondent updated its Privacy Policy on August 12th 2024 and on October 31st 2024. We attached a compare document of the Privacy Policy version of June 21st 2022 and the version of August 12th 2024 (**Annex 3B**) and of the Privacy Policy version of June 21st 2022 and the version of October 31st 2024 (**Annex 3C**).
17. AliExpress Singapore claims its Privacy Policy covers the processing activity regarding data related to the Platform the Complainant is using (**Annex 3A**; **Annex 3B**; **Annex 3C** Introduction).
18. The section "*INTERNATIONAL TRANSFERS OF PERSONDAL DATA*" of the Privacy Policy describes AliExpress' Singapore international data transfers. AliExpress does not specify the exact destination of international data transfers. According to the Privacy Policy, any personal data of the Complainant may be transferred to one of Alibaba's data centers, including data centers in China.[16] (**Annex 3A**, Section M; **Annex 3B** Section N; **Annex 3C** Section N).
19. That the Complainant's personal data is being transferred to China, is acknowledged by the fact that the section "*DISCLOSURE OR SHARING OF PERSONAL INFORMATION*" of the Respondents' Privacy Policy states: "*Alibaba group entities and affiliated companies and/or their designated service providers that work with us to provide processing services such as software, tools, systems*

[15] https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407_9_5_23227.html?spm=a1zaa.8161610.0.0.bcff7c5aiGqxhP (Privacy Policy of June 21st 2022); https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407_9_6_24275.html?spm=a1zaa.8161610.0.0.14b17c5amlWneI (Privacy Policy of August 12th 2024); https://terms.alicdn.com/legal-agreement/terms/suit_bu1_aliexpress/suit_bu1_aliexpress201909171350_82407.html (Privacy Policy of Octer 31st 2024).

[16] "*In connection with providing the services through our Platform, we will store your personal data processed through the Platform in the United States, Russia, Germany, China and/or Singapore, depending on the country you are located in.*" (**Annex 3A**, Section M); "*In connection with providing the services through our Platform, we will store your personal data processed through the Platform in the United States, Russia, Germany, China and/or Singapore, depending on the country you are located in, mainly for back up and data center storage.*" (**Annex 3B**, Section N); "*In connection with providing the services through our Platform, we will store your personal data processed through the Platform in the United States, Russia, Germany, South Korea, China and/or Singapore, depending on the country you are located in, mainly for back up and data center storage.*" (**Annex 3C**, Section N).

and messaging services for purposes described in this Privacy Policy." (**Annex 3A**, **Annex 3B**, **Annex 3C** Section C).

20. In the latest version of the Privacy Policy, the following sentence is added to this Section C: "*Please refer to Alibaba annual financial report for the group entities*." (**Annex 3C**, Section C). According to Alibaba's annual financial report of 2024, these group entities include: *Taobao and Tmall Group, Cloud Intelligence Group, Alibaba International Digital Commerce Group, Cainiao Smart Logistics Network Limited, Local Services group, Digital Media and Enternatinment Group* and others.[17] These companies are (mainly) established in China.
21. Furthermore, in this latest version of the Privacy Policy, several specific recipients are added, including: *Sesame Credit Management Co. Limited; Hangzhou Cainiao Logistics Information Technology Co. Ltd; ZhongAn Online P & C Insurance Co. Ltd.; Neusoft Cloud Technology Co. Ltd. and Hangzou Orange Shield Information Technology Co. Ltd* (**Annex 3C**, Section C). These recipients are established in China.
22. Moreover, AliExpress describes in its' Privacy Policy it has "*to make mandatory disclosures to law enforcement.*" (**Annex 3A**, **Annex 3B**, **Annex 3C**, Section J; see also Section C). Since these "lawful requests" are not limited to EU-law, these also include "lawful requests" under Chinese (intelligence service) laws.
23. AliExpress Singapore states in its Privacy Policy in section "*INTERNATIONAL TRANSFERS OF PERSONAL DATA*" (**Annex 3A**, Section M; **Annex 3B**, Section N; **Annex 3C**, Section N), that it transfers personal data outside the EEA, including China, on the basis of standard contractual clauses (SCCs), if the transfer is not subject to an adequacy decision.[18] Given the lack of any adequacy decision regarding China, AliExpress seems to rely on SCCs under Article 46 GDPR for all relevant data transfers to China.

[17] Alibaba, *Fiscal Year 2024 Annual Report*, https://data.alibabagroup.com/ecms-files/1514443390/5788a02d-696c-412a-ad2a-386d19b21769/Alibaba%20Group%20Holding%20Limited%20Fiscal%20Year%202024%20Annual%20Report.pdf, e.g. p. 18.

[18] "*There will also be international transfers of your information among the above-mentioned countries. We take appropriate steps to ensure that recipients of your personal information are bound to duties of confidentiality and we implement appropriate measures to ensure your personal information will remain protected in accordance with this Privacy Policy, such as standard contractual clauses or other mechanism provided for in the applicable law*." (**Annex 3A**, Section M); "*Where the transfer is not subject to an adequacy decision or regulations, we take appropriate steps to ensure that recipients of your personal information are bound to duties of confidentiality and we implement appropriate measures to ensure your personal information will remain protected in accordance with this Privacy Policy and applicable laws. The safeguards we use to transfer data in case of both our group companies and third party services providers for personal information originating from the EEA and UK are the European Commission's Standard Contractual Clauses, and the UK Addendum (as applicable).*" (**Annex 3B** and **Annex 3C**, Section N).

2.4. Chinese government access to AliExpress' user data

24. Neither AliExpress Singapore, nor Alibaba Group provides any information regarding Chinese government requests made to them or access given by them upon such requests.
25. However, another Chinese company, i.e. Xiaomi Inc., confirmed that they receive many requests from various Chinese public authorities regarding user data.[19] Xiaomi's Transparency Reports of 2020, 2021 and 2022 (**Annex 5**, **Annex 6** and **Annex 7**) show that the Xiaomi Group receives thousands of requests for user data from various Chinese government bodies, and these requests are almost always granted (**Annex 8**).
26. Neither AliExpress Singapore, nor Alibaba Group did publish similar transparency reports, however we note that, in particular, Chinese law grants the authorities with unrestricted powers regarding access to data processed by, inter alia, Chinese companies.[20] Thus, it is very likely that AliExpress Singapore, being a subsidiary of a Chinese company and part of the Alibaba Group, also receives a very high number of requests by Chinese government bodies and has to give access to personal data in case of such requests, since the same laws apply to them.

2.5. Second complaint

27. The Complainant is planning on filing a separate complaint regarding the violation of Article 12 and Article 15 GDPR by AliExpress Singapore. Because this Complaint and this second complaint handle different violations, they should therefore be examined and handled separately.

3. COMPETENT AUTHORITY

28. This complaint is being lodged with the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit, hereinafter: "*GBA*") because AliExpress Singapore's representative in Europe is located in Belgium.
29. As mentioned in Section 2.1 above, based on widely available public reporting, the Complainant assumes that the Respondent's main establishment within the EU is located in Belgium. A facility located in the Belgian city of Liège (a subsidiary of Alibaba Group, called Cainiao Smart Logistics Network Limited,[21] also known as AliExpress' European hub or Cainiao Liège eHub[22]) is responsible for managing

[19] E.g. Xiaomi Transparency Report GOVERNMENT REQUESTS FOR USER INFORMATION January 1 – December 31, 2022, link, p. 4-7 (**Annex 6**).

[20] Wang, Zhizheng, 'Systematic Government Access to Private-Sector Data in China', in Fred H. Cate, and James X. Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford: 2017); EDPS Government access to data in third countries, EDPS/2019/02-13, link.

[21] https://www.alibabagroup.com/en-US/about-alibaba-businesses; https://global.cainiao.com/

[22] https://www.linkedin.com/showcase/cainiao-liege-ehub/

purchases of European clients of AliExpress Singapore.[23] While there may be other smaller sales offices of Alibaba in Europe, there is no indication of any similar, let alone larger, establishment than the hub in Liège or any decision-making as to the purposes of means of processing in Europe.

30. Therefore, the Cainiao Smart Logistics Network Limited in Liège should be treated as the Respondent's representative in the Union under Article 27(1) GDPR. Because of this, we consider the GBA to be the the competent authority to handle this Complaint.

4. VIOLATIONS OF THE GDPR

4.1. Violation of Chapter V GDPR

31. According to AliExpress' Singapore Privacy Policy, the Complainant's personal data is being transferred to China by AliExpress Singapore: "[…] *we will store your personal data processed through the Platform in* […] *China* […]. […] *There will also be international transfers of your information among the above-mentioned countries*." (**Annex 3A**, Section M; **Annex 3B**, Section N; **Annex 3C**, Section N).
32. According to Article 44 GDPR, any transfer of personal data to a third country is, in principle, forbidden. A transfer may take place only if the conditions laid down in Chapter V are complied with. As explained below, none of these conditions are met, and therefore, the transfer of personal data of the Complainant to China by the Respondent is unlawful because of the following:

4.1.1 No adequacy decision (Article 45 GDPR)

33. The EU Commission has not decided that China ensures an adequate level of protection (cf. Article 45(1) GDPR). Therefore, AliExpress' Singapore cannot transfer personal data of the Complainant to China on the basis of an adequacy decision.
34. Because of this, according to its Privacy Policy, AliExpress' Singapore transfers personal data on the basis of the EU Commission's standard contractual clauses (hereinafter: "*SCCs*") (Article 46(2)(c) GDPR): "*Where the transfer is not subject to an adequacy decision* […] [t]*he safeguards we use to transfer in case of both our group companies and third party service providers* […] *are the European Commission's Standard Contractual Clauses* […]." (**Annex 3A**, Section M, **Annex 3B**, Section N; **Annex 3C**, Section N).

[23] https://www.ft.com/content/256ee824-9710-49d2-a8bc-f173e3f74286 ; https://www.reddit.com/r/Aliexpress/comments/lvayiu/why_is_everything_coming_to_europe_being_sent_to/?rdt=49110; https://www.belganewsagency.eu/belgian-intelligence-monitors-alibaba-hub-over-espionage-concerns

35. This means the Respondent has to conduct a data transfer impact assessment (hereinafter: "*TIA*"), to verify whether Chinese laws or practices impinge on the effectiveness of the SCCs under Article 46 GDPR:[24]

4.1.2 Chinese law impinges the effectiveness of appropriate safeguards

4.1.2.1 "Essentially equivalent level of data protection" requirement

36. According to Article 44 GDPR, data transfers to countries outside of the EEA – such as China – are only allowed when "*the level of protection of natural persons guaranteed by this Regulation is not undermined.*"
37. The CJEU clarified that it is the European Commission's task to evaluate the level of data protection in a third country in case of an adequacy decision under Article 45 GDPR.[25] Nevertheless, the controller who relies upon appropriate safeguards under Article 46 GDPR – such as SCCs – also needs to verify to what extent the third country law satisfies a data protection level equivalent to the EU level of data protection.[26]
38. According to the CJEU and Article 46(1) GDPR, for a third country's level of data protection to be considered as essentially equivalent in relation to appropriate safeguards, a third country's laws must (at least) under Article 7, 8 and 47 CFR:

    (a) Provide data subjects (the Complainant) with enforceable data protection rights;
    (b) Provide data subjects (the Complainant) with effective legal remedies;
    (c) Guarantee the limitation of access to personal data (of the complainant) by law enforcement and national security authorities.[27]

4.1.2.2 Violation of Article 7 and 8 CFR

(A) Commercial data transfers

[24] Cf. EDPB Recommendations 2020/01, Section 2.3: "*Section 2.3 Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer*".
[25] CJEU C-363/14 (*Schrems I*), CJEU C-293/12 and C-594/12 - Digital Rights Ireland.
[26] CJEU C-363/14 (*Schrems I*), para. 73 and para 101-102. The CJEU clarified that the concept of essential equivalence is not about the exact copy of the EU data protection law, but it: "[…] *must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter*."; Cf. EDPB Recommendations 2020/01, para. 32: "*You will need to look into the characteristics of each of your transfers and determine whether the domestic legal order and/or practices in force of the country to which data is transferred (or onward transferred) affect your transfers*."
[27] CJEU C-311/18 (*Schrems II*), para 103-105; WP29 Adequacy Referential, WP254rev.01, Chapter 4 (endorsed by the EDPB: link , under 15.).

39. According to AliExpress Singapore, the basis of the transfer of personal data of the Complainant to China are SCCs (**Annex 3A**, Section M; **Annex 3B**, Section N; **Annex 3C**, Section N). We would like to note that, in principle, the SCCs only cover commercial data transfers, i.e. date transfers related to the purchases concluded via the Platform.
40. Because of their nature, the SCCs do not cover relations between the controller and third-country authorities. Therefore, the effectiveness of SCCs can be severely compromised by the third-country law.

(B) Access to personal data by law enforcement and national security authorities

41. Some commentators mention the close alignment of Chinese data protection law (in general) with the European or American data protection law.[28] In reality, however, the Chinese Cybersecurity Law (hereinafter: "*CSL*"),[29] the Chinese Personal Information Protection Law (hereinafter: "*PIPL*"),[30] the Chinese Civil Code,[31] and the Chinese Data Security Law (hereinafter: "*DSL*")[32] differ substantially from European laws.[33]
42. First, Chinese data localisation laws make it obligatory to store data that was "*collected and produced*" and "*collected and generated*" in China within Chinese

[28] E. Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU?', *Penn State Journal of Law and International Affairs* 2020/8, p. 53–54, 81–82; R. Berti, 'Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union', *European Journal of Privacy Law & Technologies* 2020/34, p. 37.

[29] Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 11 July 2016, came into force on 1 June 2017).

[30] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 20 August 2021, came into force on 1 November 2021).

[31] Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of of the People's Republic of China] (issued by the National People's Congress on 28 May 2020, came into force on 1 January 2021);

[32] Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 10 June 2021, came into force on 1 September 2021).

[33] D. Hanlin, 'The System Position and Protection of Personal Information Right in General Provisions of the Civil Law', *US-China Law Review* 2018/3, p. 153–154; B. Qu, C. Huo, 'Privacy, National Security, and Internet Economy: An Explanation of China's Personal Information Protection Legislation', *Frontiers of Law in China* 2020/3, p. 364; E. Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU?', *Penn State Journal of Law and International Affairs* 2020/8, p. 53–54; Y. Shao, 'Personal Information Protection: China's Path Choice', *US-China Law Review* 2021/18, p. 236–238.

territory.[34] Therefore, all data controllers[35] running their business activity (partially) in China – like companies within the Alibaba Group – fall under the duty to store data created in China locally.[36] Because of this, practically any transfer of personal data from Chinese territory abroad (to the EU/EEA) requires prior authorization under the Cyberspace Administration of China Data Transfer Guidelines.[37]

43. Legal literature indicates the Cyberspace Administration of China (hereinafter: "*CAC*") (also known as the State Internet Information Department) has discretionary power over every data transfer authorisation decision.[38] As a result,

---

[34] **Article 37 Cybersecurity law of the People's Republic of China (CSL)**: "*Personal information and important data collected and produced by critical information infrastructure operators during their operations within the territory of the People's Republic of China shall be stored within China. If it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration in conjunction with relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.*" (emphasis added)
[关键信息基础设施的运营者在中华人民共和国 境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业 务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关 部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其 规定。].
Article 40 Personal Information Protection Law of the People's Republic of China (PIPL): "*Critical information infrastructure operators and the personal information processors that process the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall store domestically the personal information collected and generated within the territory of the People's Republic of China. Where it is truly necessary to provide the information to an overseas recipient, the security assessment organized by the national cyberspace administration shall be passed. Where laws, administrative regulations, or provisions issued by the national cyberspace administration provide that security assessment is not required, such provisions shall prevail.*" (emphasis added)
[关键信息基础设施运营者和处理个人信息达到国家 网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内 收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国 家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可 以不进行安全评估的，从其规定]

[35] That is the conclusion that may be drawn from **Article 31 CSL**: "*The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the critical information infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the critical information infrastructure that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council. The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.*" (emphasis added)
[国家对公共通信和信息服务、能源、交通、水 利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭 到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民 生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础 上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由 国务院制定。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础 设施保护体系].

[36] G. Greenleaf, S. Livingston: PRC's new data export rules: 'Adequacy with Chinese characteristics?', *University of New South Wales Law Research* Series 2017/69, p. 3–4.

[37] Shuju Chujing Anquan Pinggu Banfa (数据出境安全评估办法) [Outbound Data Transfer Security Assessment Measures] (issued by the Chinese Administration of Cyberspace on 7 July 2022, came into force on 1 September 2022), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

[38] G. Greenleaf, 'China Issues a Comprehensive Draft Data Privacy Law', *Privacy Laws & Business International Report* 2020/168, p. 12; G. Greenleaf, 'China's Completed Personal Information Protection Law: Rights Plus Cyber-security', *Privacy Law & Business International Report* 2021/20-23 p. 4.

data subjects' access requests and data portability rights become illusionary because these rights are subject to "discretional approval".

44. Second, there is a very high risk that Chinese authorities will request and obtain (unlimited) access to personal data processed by Chinese companies.[39] Chinese data protection laws do not limit the access by these authorities in any way. In fact, it is even unclear whether state authorities – including intelligence services – are covered by the definition of data controller in the PIPL and therefore if they have to comply with the PIPL.[40] Even if they do fall within the scope of the PIPL, it is unlikely, according to legal scholars, that the Chinese authorities would in practice comply with the data protection principles and other obligations of data controllers.[41]
45. Chinese laws, such as the National Security Law (hereinafter: "*NSL*"),[42] and the National Intelligence Law (hereinafter: "*NIL*")[43] but also the DSL,[44] are treated as a general legal basis for Chinese authorities' to obtain access to any personal data.[45] The general and vague nature of the provisions of the DSL, the NSL and the NIL prove that Chinese authorities can obtain unrestricted and unlimited access to personal data without providing any safeguards for the data subjects. For example:

[39] Cf. concerns raised by Belgian authorites over alleged espionage activity of Alibaba in Europe (Link).

[40] R. Creemers, 'China's Emerging Data Protection Framework', *Journal of Cybersecurity* 2022/8, p.19.; Y-J. Chen, C-F. Lin, H-W. Liu, '"Rule of Trust": The Power and Perils of China's Social Credit Megaproject', *Columbia Journal of Asian Law* 2021/32, p. 27; Y. Duan, 'Balancing the Free Flow of Information and Personal Data Protection', 3 April 2019, https://ssrn.com/abstract=3484713, p. 11–12; L. Yu, B. Ahl, 'China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform', *Journal Hong Kong Law Journal* 2021/51, p. 292.

[41] G. Greenleaf, 'China's Completed Personal Information Protection Law: Rights Plus Cyber-security', *Privacy Law & Business International Report* 2021/20-23, p. 2; R. Creemers, 'China's Emerging Data Protection Framework', *Journal of Cybersecurity* 2022/1, p. 14; C. You, 'Half a Loaf is Better than None: The New Data Protection Regime for China's Platform Economy', *Computer Law & Security Review* 2022/45, p. 19; Q. Zhou, 'Whose Data Is It Anyway? An Empirical Analysis of Online Contracting for Personal Information in China', *Asia Pacific Law Review* 2023/31, p. 90; L. Zheng, 'Personal Information of Privacy Nature under Chinese Civil Code', *Computer Law & Security Review* 2021/43, p. 7; R. Creemers, 'China's Emerging Data Protection Framework', *Journal of Cybersecurity* 2022/1, p. 19; G. Greenleaf, S. Livingston, 'China's New Cybersecurity Law – Also a Data Privacy Law?', *Privacy Laws & Business International Report* 2016/19, p. 3.

[42] Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [the National Security Law of People's Republic of China] (issued by the Standing Committee of the National People's Congress on 1 July 2015, came into force on 1 July 2015).

[43] Zhonghua Renmin Gongheguo Guojia Qingbao Fa (中华人民共和国国家情报法) [the National Intelligence Law of People's Republic of China] (issued by the Standing Committee of the National People's Congress on 27 April 2018, came into force on 27 April 2018).

[44] Article 35 DSL.

[45] EDPS *Government access to data in third countries*, EDPS/2019/02-13; Human Rights Watch: Letter to House Committee on Energy and Commerce,16 March 2023, https://www.hrw.org/sites/default/files/media_2023/03/Letter%20to%20House%20Committee%20on%20TikTok%20-%20web.pdf; T. Giladi Shtub, M.S. Gal, 'The Competitive Effects of China's Legal Data Regime', *Journal of Competition Law and Economics* 2022/4, p. 11.

(a) Article 35 DSL: "*As needed for maintaining national security or investigating crimes, a public security authority or national security authority shall legally pull data in accordance with relevant provisions issued by the state and by strictly following approval procedures, and the relevant organizations and individuals shall provide cooperation*."[46] It should be noted that Article 35 DSL uses an unspecified term of "pulling data", which suggests that the authorities can access all the (personal) data available to a data controller, including personal data that is being processed outside of China.[47] (emphasis added)

(b) Article 11 NSL: "*All citizens of the People's Republic of China, state authorities, armed forces, political parties, people's groups, enterprises, public institutions, and other social organizations shall have the responsibility and obligation to maintain national security*".[48] (emphasis added)

46. As a result, the processing by Chinese national law enforcement and/or national security authorities is not based on clear, precise and accessible rules, necessity and proportionality with regard to legitimate interests pursued are not demonstrated, the processing is not subject to independent supervision and there are no effective remedies available to the Complainant (or other EU data subjects).[49]
47. The Transparency Reports of Xiaomi (**Annex 5**; **Annex 6**; **Annex 7** and **Annex 8**) also confirm the very high risk of Chinese authorities requesting and obtaining (unlimited) access to personal data in practice (cf. Section 2.4 of this Complaint). These Transparency Reports of Xiaomi show that:

(a) Chinese authorities request access to personal data on a very large scale, while in the same years Xiaomi only received few requests to provide personal data of Xiaomi users to EU/EEA authorities.

(b) Xiaomi almost always complies (or has to comply) with these Chinese authorities' requests.

48. Although AliExpress Singapore and/or Alibaba Group have not published any reports on Chinese authorities' data requests, Xiaomi reports provide solid

[46] [公安机关、国家安全机关因依法维护国家安全 或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的 批准手续，依法进行，有关组织、个人应当予以配合].
[47] See by analogy with the US Cloud Act: https://www.justice.gov/criminal/cloud-act-resources
[48] 第十一条: 中华人民共和国公民、一切国家机关和武装力量、 各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家 安全的责任和义务.
[49] WP29 Adequacy Referential, WP254/01 (endorsed by the EDPB: link, under 15), p. 9.

evidence of such requests with respect to personal data processed by China-based companies in general.

4.1.2.3 Violation of Article 47 CFR

49. It is almost impossible for a foreign data subject to exercise his/her rights under the PIPL[50] or the Chinese Civil Code.[51]
50. First, there is no dedicated, independent and competent data protection authority in China.[52] The CAC plays an important role in Chinese data protection law,[53] although for some provisions it is very difficult to indicate which authority is actually responsible for a particular task.[54] It is worth emphasising that the CAC is closely related to the State Council,[55] and as such may pursue political goals rather than effective independent supervision of data processing activities.
51. Second, an overall assessment of the Chinese judicial system, leads to the conclusion that the judicial control over data processing activities in China is very limited. The World Justice Project Rule of Law Index ranked Chinese courts on the 139th position (out of 142 countries) within the category of fundamental rights protection[56] and the 132nd position in category of restraints imposed by the courts on government powers.[57] When it comes to data protection, Chinese courts are not free from political pressure. As a result, the current political needs may prevail over the rights and freedoms of the data subjects.[58] This impossibility extends to

[50] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 20 August 2021, came into force on 1 November 2021).

[51] Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of of the People's Republic of China] (issued by the National People's Congress on 28 May 2020, came into force on 1 January 2021); Q. Zhou, 'Whose Data Is It Anyway? An Empirical Analysis of Online Contracting For Personal Information in China', Asia Pacific Law Review 31(1) (2023), p. 89; B. Zhao, G.P. Mifsud Bonnici, '*Protecting EU Citizens' Personal Data in China: A Reality or a Fantasy?*', *International Journal of Law and Information Technology* 2016/126, p. 132, 135–139; J. Huang, 'Reciprocal Recognition and Enforcement of Foreign Judgments in China: Promising Developments, Prospective Challenges and Proposed Solutions', *Nordic Journal of International Law* 2019/88; M. Douglas, V. Bath, M. Keyes & A. Dickinson (Eds), *Commercial Issues in Private International Law: A Common Law Perspective*. Oxford: Hart Publishing: 2019, p. 142; J. Wang, 'Dispute Settlement in the Belt and Road Initiative: Progress, Issues, and Future Research Agenda', *The Chinese Journal of Comparative Law* 2020/1, p. 13-14.

[52] G. Greenleaf, S. Livingston, 'China's New Cybersecurity – Also a Data Privacy Law?', *Privacy law & Business International* Report 2016/144, p. 8

[53] W. Chaskes: 'The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet', *Washington & Lee Law Review* 2022/1169, p. 1175; C. Wang, J. Zhang, N. Lassi et al, 'Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective', *Healthcare* 2022/10, p. 4; C. You, 'Half a Loaf is Better than None: The New Data Protection Regime for China's Platform Economy', *Computer Law & Security Review* 2022/45, p. 21.

[54] R. Creemers, 'China's Emerging Data Protection Framework', *Journal of Cybersecurity* 2022/8, p. 14.

[55] G. Pyo, 'An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts', *Columbia Journal of Transnational Law* 2021/1, p. 236.

[56] The World Justice Project Rule of Law Index (link).

[57] The World Justice Project Rule of Law Index (link).

[58] H. Dorwart, 'Platform Regulation from the Bottom up: Judicial Redress in the United States and China', *Policy & Internet* 2021/14, p. 378; A.S. Sweet, C. Bu, 'Breaching the Taboo? Constitutional Dimensions of

obtaining effective administrative or judicial redress or claiming compensation as a data subject under the PIPL or the Chinese Civil Code.[59]

52. Third, when Chinese law enforcement or national security authorities request access to personal data, these Chinese authorities follow the "black box" route,[60] making it impossible for a data subject, to understand how exactly such requests have been or will be granted.[61] This makes it impossible to exercise any data protection rights in this regard.
53. Fourth, the scope and application of Chinese data protection laws are unclear. Chinese data protection provide rights to data subjects, but it is unclear whether and to what extent these rights can be exercised in practice. There are no provisions explaining the relationship between the CSL, the PIPL, the Chinese Civil Code and the DSL. As a result, all of them potentially apply and only a factual, case-by-case assessment should determine which law covers a particular data processing.[62] However, this leads to a situation where data controllers do not specify which law or laws apply or applies to the data processing or do so without any explanation. Therefore, it is also unclear whether and to what extent, data subjects can exercise and/or enforce their rights.[63]

4.1.3 Conclusion: AliExpress Singapore violates Chapter V GDPR

54. It is then a foregone conclusion that any assessment of Chinese law, in particular the assessment that needs to be performed by the Respondent transferring

China's New Civil Code', *Asian Journal of Comparative Law* 2023/3, p. 11

[59] Q. Zhou, 'Whose Data Is It Anyway? An Empirical Analysis of Online Contracting For Personal Information in China', *Asia Pacific Law Review* 31(1) (2023), p. 89; B. Zhao, G.P. Mifsud Bonnici, 'Protecting EU Citizens' Personal Data in China: A Reality or a Fantasy?', *International Journal of Law and Information Technology* 2016/126, p. 132, 135–139; J. Huang, 'Reciprocal Recognition and Enforcement of Foreign Judgments in China: Promising Developments, Prospective Challenges and Proposed Solutions', *Nordic Journal of International Law* 2019/88. M. Douglas, V. Bath, M. Keyes & A. Dickinson (Eds), *Commercial Issues in Private International Law: A Common Law Perspective*. Oxford: Hart Publishing: 2019, p. 142; J. Wang, 'Dispute Settlement in the Belt and Road Initiative: Progress, Issues, and Future Research Agenda', *The Chinese Journal of Comparative Law* 2020/1, p. 13-14

G. Greenleaf, S. Livingston, 'China's New Cybersecurity – Also a Data Privacy Law?', *Privacy law & Business International* Report 2016/144, p. 8

[60] W. Chaskes, 'The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet', *Washington & Lee Law Review* 2022/1169, p. 1182.

[61] D. Gershgorn, 'China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space The program turns neighbors into agents of the surveillance state', OneZero, 2 March 2021, https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015; B. Zhao, F. Yang, 'Mapping the development of China's data protection law: Major actors, core values, and shifting power relations', *Computer Law and Security Review* 40(1) 2021, p. 3–4; E. Feng, ''Surveillance State' Explores China's Tech and Social Media Control Systems', 7 September 2022, https://www.npr.org/2022/09/07/1118105165/surveillance-state-explores-chinas-tech-and-social-media-control-systems.

[62] P. Cai, L. Chen, 'Demystifying Data Law in China: A Unified Regime of Tomorrow', *International Data Privacy Law* 2022/5, p. 79.

[63] L. Du, M. Wang, 'Genetic Privacy and Data Protection: A Review of Chinese Direct-to-Consumer Genetic Test Services', *Frontiers of Law in China* 2020/11, p. 6.

personal data to China on the basis of appropriate safeguards (SCCs) under Article 46 GDPR, should result in avoiding, suspending and/or terminating the data transfers to China to avoid compromising the level of data protection of the personal data.[64]

55. Article 44 GDPR requires AliExpress Singapore not to transfer the Complainant's personal data to China, unless it provides the Complainant with one of the appropriate safeguards under Article 46 GDPR, such as SCCs, supplemented by necessary, additional safeguards.[65] However, the Complainant is not aware of any supplemental measures taken by the Respondent, nor of any supplemental measures that could overcome the problematic legislation and the non-equivalent level of data protection.[66]

5. APPLICATIONS

56. As a consequence, and given that the transfer of the Complainant's personal data to China and the processing of the Complainant's personal data in China **is ongoing**, we request that the GBA takes (among others) the following urgent actions:

- *First*, fully investigate the matter under Article 58(1) GDPR.
- *Second*, **immediately order the suspension of data flows to China** under Article 58(2)(j) GDPR regarding the transfer of the Complainant's and other European users' data to China as it does not provide essentially equivalent level of data protection under Article 44 and 46 GDPR.
- *Third*, bring its **data processing activities into compliance with Chapter V of the GDPR** under Article 58(2)(d) GDPR.
- *Fourth,* issue an **effective, proportionate and dissuasive fine** under Article 58(2)(i) and Article 83 GDPR.

5.1. Duty to act

57. The CJEU has repeatedly held that supervisory authorities have a positive duty to act if they are made aware of a GDPR violation. In C-311/18 *Schrems II* the CJEU held at paragraph 111:

> *"In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the*

[64] Cf. EDPB Recommendations 01/2020, para 72.
[65] CJEU C-311/18 (*Schrems II*), para. 101-104.
[66] EDPB Recommendations 01/2020, para 75.

view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt."

58. In the Joint Cases C-26/22 and C-64/22 *SCHUFA* the CJEU has further highlighted at paragraph 57:

    "In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. Where, following its investigation, such an authority finds an infringement of the provisions of that regulation, it is required to react appropriately in order to remedy the shortcoming found. To that end, Article 58(2) of that regulation lists the various corrective measures that the supervisory authority may adopt."

59. In C-768/21 *Land Hessen*, the AG has further issued an opinion saying at paragraph 82:

    "[...] *that the supervisory authority has an obligation to act when it finds a personal data breach in the course of investigating a complaint. In particular, it is required to define the most appropriate corrective measure(s) to remedy the infringement and ensure that the data subject's rights are respected.* [...]"

60. An equal result can be derived from the general duty of public authorities to uphold fundamental rights - like the right to data protection in Article 8 of the Charter. There is consequently no question that the GBA has a duty to act in this case.

5.2. Investigation under Article 58(1) GDPR

61. Given that some of the details of the processing of the Complainant's personal data by AliExpress Singapore are unclear, we hereby request a full investigation of the GBA using all powers under Article 58(1) GDPR, which should include at least the following steps:

- Clarification of the specific destination(s) of the Complainant's personal data transferred internationally (globally).
- Clarification of the exact legal basis for the transfer of the Complainant's personal data from the EEA to third countries, in particular to China.
- Clarification of the exact relationship between AliExpress Singapore and Alibaba Group, (and therefore the roles of the parties), in particular with regard to the processing of the Complainant's personal data by Alibaba Group.

- Obtaining the "Transfer Impact Assessment", or any documents or communications relating thereto, that AliExpress Singapore should have conducted pursuant to Article 46(1) GDPR, including any supplementary measures taken by AliExpress Singapore.

- Obtaining the record of processing activities under Article 30 GDPR.

5.3. Corrective powers under Article 58(2)(d)(j) GDPR

62. Even before any investigation may have come to a final conclusion, we urge the GBA to already take imminent, preliminary steps to ensure that AliExpress Singapore does not pursue the processing operations any further, including but not limited to:

    (a) Order a suspension of transfer of personal data of Complainant and other European AliExpress Singapore services' users to China, under Article 58(2)(j) GDPR;

    (b) Order AliExpress Singapore to bring the processing into compliance with Chapter V of the GDPR under Article 58(2)(d) GDPR;

63. Additionally, the Complainant also requests the GBA to state:

    (a) That SCCs are not an appropriate basis for AliExpress Singapore to transfer the Complainant's personal data to China;

    (b) That the transfers of the Complainant's personal data to third countries by AliExpress Singapore are unlawful.

5.4. Fine under Article 58(2)(i) and Article 83 GDPR

64. It is our view that that AliExpress Singapore has breached (at least) Articles 44; 45(1) and 46(1) GDPR in a manner that amounts to a clear and intentional breach of the law – particularly in the light of the long list of previous CJEU decisions, EDPB recommendations and decisions by national data protection authorities.
65. Therefore, we suggest that the GBA to impose a fine on AliExpress Singapore in accordance with Article 58(2)(i) GDPR. We note that Article 83(1) GDPR requires the GBA to impose fines that are "*effective, proportionate and dissuasive*".

6. CONTACT

66. Communications between *noyb* and the GBA in the course of this procedure can be done by email at [redacted] with reference to the **Case-No C093-01** or [redacted].