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

Garante per la protezione dei dati personali
Piazza Venezia 11
00187 Roma, Italia

Via email: protocollo@gpdp.it

Vienna, 16 January 2024

noyb Case-No: **C093-02**

Complainant: [redacted]

SHEIN nickname: [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: **Roadget Business Pte. Ltd.**
12 Marina Boulevard, #15-01, Marina Bay Financial Centre, Singapore 018982, 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 ("SHEIN")

3. The Respondent is a "*global fashion and lifestyle e-retailer*", according to its website.[1] More specifically, the Respondent provides users with access to an e-commerce platform called SHEIN, on which users can purchase a variety of goods, such as clothing, shoes and beauty products (hereinafter: "*Platform"*). According to SHEIN's website, the SHEIN app is one of the most downloaded apps in the world.[2]
4. SHEIN was founded in 2012 in China, but to be accessible worldwide, the SHEIN Group acts (or claims to act) via its subsidiaries, such as Roadget Business Pte. Ltd (SHEIN's headquarters in Singapore) (the Respondent), Infinite Styles Ecommerce Co. Limited (in Ireland), Zoetop Business Co. Limited (in Hong Kong), Guangzhou SHEIN International Import & Export Co. Ltd. (in China), etcetera. Even though SHEIN's headquarters are in Singapore, one of SHEIN's "*key centers*" is still established in Southern China.[3]
5. The Platform serves customers worldwide, including customers in the EEA/EU. By offering its Platform to EU/EEA users, the Respondent 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 the Respondent 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 (**Annex 3**, e.g. under 1.).[4]

---

[1] "*SHEIN is a global fashion and lifestyle e-retailer committed to making the beauty of fashion accessible to all.*" https://eur.shein.com/About-US-a-117.html

[2] *"The SHEIN app is one of the most downloaded apps in the U.S. and the world. It is the primary way customers can explore all SHEIN has to offer."* https://www.sheingroup.com/about-us/our-global-presence/

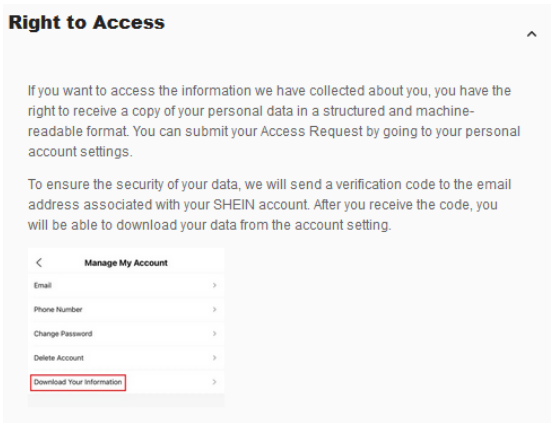
[3] *"Headquartered in Singapore, SHEIN serves customers in 150+ countries from key centers of operation around the world, including the U.S., Brazil, Ireland, and Southern China."* https://www.sheingroup.com/about-us/our-global-presence/

[4] **Annex 3**, e.g. Section 1: "*Pursuant to the EU General Data Protection Regulation ("GDPR"), personal information in this Policy is referred to as "personal data" as defined in the GDPR, and in this Policy can be interchangeably used with the term "personal information." For residents of the European Union, "personal data" is any information that alone or in combination with other information, identifies or makes an individual identifiable."*

6. SHEIN claims that for all data processing of EEA/EU customers, Infinite Styles Ecommerce Co. Limited in Ireland is the controller and is "*operating the SHEIN Site and App*" (**Annex 3**, first paragraph) (see also paragraph 3 of this Complaint).

2.2. Complainant

7. The Complainant is a user of the SHEIN e-commerce Platform. To use the Platform and to buy products on the Platform, the Complainant had to create an account and provide personal data. According to the Privacy Policy of the Platform, the Platform collects and processes personal data, such as identity and contact information (such as an e-mail address, name, phone number), profile data (such as style preference), transaction details (such as return and refund details), location data and data about platform usage, etcetera (**Annex 3,** under 1.).
8. 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 SHEIN. For that purpose, SHEIN's website directed her to her personal account settings,[5] where she could download a copy of her personal data after SHEIN had sent her a verification code (**Screenshot 1; Annex 4A**). After downloading the file, it turned out that SHEIN provided the Complainant only with a limited list of personal data processed by SHEIN (**Annex 4B**), including her preferences, email address, nick name, but without it including any information regarding data transfers.



Screenshot 1. The Complainant received a limited list of personal data after clicking on "Download Your Information".[6]

9. Since downloading a copy of her personal data did not provide the Complainant with any information under Article 15(1)(2) or (3) GDPR about the data transfers to third countries, data location or any other information about the data processing (other than the very limited list that was provided to her (**Annex 4B**)),

[5] https://m.shein.com/eur/Privacy-Center-a-1045.html?lang=eur
[6] https://m.shein.com/eur/Privacy-Center-a-1045.html?lang=eur

she decided to file an access request under Article 15 GDPR on [redacted] 2024 (**Annex 5A**). The access request was sent to privacy@sheingroup.com, the e-mail address provided in the Respondent's Privacy Policy (**Annex 3**, under 10.).

10. The Respondent sent an "*automated reply*" to this access request of the Complainant on [redacted] 2024 (**Annex 5B**). On the [redacted] 2024 the Respondent got back to the Complainant with a request to verify her email address for the fulfilment of her access request.
11. On the [redacted] 2024 the Respondent replied to the Complainant in relation to her request (**Annex 5C**). Their reply referred to a "*data portability*" request by the Complainant and included an Excel sheet with information that was even more limited than the information that the Complainant received through the "*Download Your Information*" feature.
12. Therefore, the Complainant's questions regarding data transfers to China or any other third country by SHEIN were not answered.

2.3. SHEIN's Privacy Policy

13. Since the Complainant's habitual residence is located within the EU/EEA, SHEIN's Privacy Policy for European users applies, which is also accessible in Italian (**Annex 3**).[7] When the Complainant sent the access request to the Respondent on [redacted] 2024 (**Annex 5A**), the version of September 25, 2023 of the Privacy Policy was applicable (**Annex 3**).
14. SHEIN claims its Privacy Policy covers the processing activity regarding data related to the Platform the Complainant is using (**Annex 3,** Introduction).
15. The section "*Transfer of Your Personal Data*" (Section 9) of SHEIN's Privacy Policy describes SHEIN's international data transfers. SHEIN does not specify the exact location of international data transfers. However, according to the Privacy Policy, any personal data of the Complainant may be transferred to outside of the European Union, including to China.[8] (**Annex 3**, under 9.).
16. That the Complainant's personal data is being transferred to China, is acknowledged by the fact that the section "*Sharing Your Personal Data*" (Section 2) of SHEIN's Privacy Policy states:

> "*The Company is part of a corporate organization that has several legal entities, business processes, management structures, and technical systems. We may share your personal information with our related group companies and, in some cases, other affiliates of our corporate group*. […]." (**Annex 3**, under 2A.).

[7] https://m.shein.com/eur/Right-to-Access-a-1047.html?lang=eur

[8] "*When you access or use our Services,* ***your personal data may be processed or transferred outside the European Union, including to the United States, China and/or Singapore***. […]." (**Annex 3,** under 9.).

As described in paragraph 2.1, several companies within the SHEIN Group are established in China.

17. Furthermore, SHEIN's Privacy Policy describes SHEIN complies with: "*lawful requests from a competent law enforcement agency or court.*" (**Annex 3**, Section 1.1 under "*To comply with legal or compliance requirements*"), and:

> "*We have the right to disclose your personal information for compliance with a legal obligation, or when we believe that disclosure is necessary to protect our rights and/or comply with a judicial proceeding, court order, request from a regulation, or any other legal process serves on us* […]." (**Annex 3**, under 2D.)

Since these "lawful requests" and "legal or compliance requirements" are not limited to requests under EU-law, these also include "lawful requests" and "legal or compliance requirements" under Chinese (intelligence service) laws.

18. SHEIN states in its Privacy Policy that it transfers personal data outside the European Union, including China, on the basis of "*appropriate safeguards such as Standard Contractual Clauses and/or we transfer the personal information pursuant to Article 49(1)(b) GDPR.*" (**Annex 3**, Section 9).

2.4. Chinese government access to SHEIN's user data

19. Neither the Respondent, nor the SHEIN Group provides any information regarding Chinese government requests made to them or access given to personal data of users by them upon such requests.
20. However, the Chinese company, Xiaomi Inc., confirmed that they receive many requests from various Chinese public authorities regarding user data.[9] Xiaomi's Transparency Reports of 2020, 2021 and 2022 (**Annex 6**, **Annex 7** and **Annex 8**) show that the Xiaomi Group receives thousands of requests regarding user data from various Chinese government bodies, and these requests are almost always granted (**Annex 9**).
21. Neither the Respondent, nor SHEIN 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.[10] Thus, it is very likely that the Respondent, being a subsidiary of a Chinese company and part of the SHEIN 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.

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

[10] 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.

2.5. Second complaint

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

3. COMPETENT AUTHORITY

23. SHEIN claims that for all data processing of EU customers, Infinite Styles Ecommerce Co. Limited in Ireland is the controller and they claim Infinite Styles Ecommerce Co. Limited in Ireland is "*operating the SHEIN Site and App*" (**Annex 3**, first paragraph).
24. However, on the address where Infinite Styles Ecommerce Co. Limited is registered – 1-2 Victoria Buildings, Haddington Road, Dublin 4 (**Annex 3**, Section 10) – at least 628 other companies are registered as well, including but not limited to the CSC Services[11], Shopify and law firm Mishcon de Reya Representative Services (Europe) Limited (hereinafter: "*Mishcon de Reya*").[12]
25. It is hard to believe that in the small building on 1-2 Victoria Buildings, Haddington Road, Dublin 4, 630 companies are actually established there. Arguably, it even seems hard to fit the claimed 30 tech employees of SHEIN in there, especially since there is a coffee shop or café taking up a significant chunk of the property already.[13]
26. A German report also alleges that SHEIN's Dublin office is only created to pay less tax, while the "e-commerce" – and therefore also the purposes and means of the processing – are still decided on from SHEIN's main headquarters:

> *„Der Hauptsitz ist im Besitz von Zoetop Business in Hong Kong. Diese Firma verwaltet auch die internationalen Markenrechte der Shein-Gruppe und das E-Commerce-Geschäft. Zoetop wiederum gehört der Beauty of Fashion Investment auf den British Virgin Islands, bekannt als undurchsichtiger Finanzplatz. Mit den britischen Cayman Islands, Delaware in den USA und Dublin in Irland haben auch andere Shein-Firmen ihren Sitz in Steueroasen."*[14]
>
> *„The head office is owned by Zoetop Business in Hong Kong. Kong. This company also manages the Shein Group's international rights of the Shein Group and the e-commerce business. business. Zoetop, in turn, is owned by Beauty of Fashion Investment in the British Virgin Islands, known as an opaque financial centre. With the British Cayman*

[11] https://www.cscglobal.com/service/about/csc-office-locations/ireland/

[12] There are at least 628 companies with the same Eircode: https://www.vision-net.ie/Company-Info/Mishcon-De-Reya-Representative-Services-Europe-Limited-685267. An Eircode is Ireland's postcode system and it consists of a seven-character alphanumeric postcode. Each Eircode is unique to a postal address and its geographic location.

[13] https://estatecreate.com/victoriabuildings/en/page_82536.php

[14] https://www.publiceye.ch/fileadmin/doc/Magazin/2021-11_PublicEye_Magazin_Nr32_D_72dpi.pdf, p. 4.

Islands Islands in the UK, Delaware in the USA and Dublin in Ireland other Shein companies are also based in tax havens." (auto translation)

27. Furthermore, it's striking that the Mishcon de Reya offers an "*EU Representative service*" to companies. This "*EU Representative service*" mainly seems to involve "offering" companies a "letterbox" as a "main establishment" within the EU:

> "*While you could set up an office in the appropriate location(s) and employ a local representative yourself, there is an easier way that saves you time and provides peace of mind: Assign, our EU/UK representative subscription service.* [...] *Our entity that provides the EU Representative services is located in Ireland.*"[15]

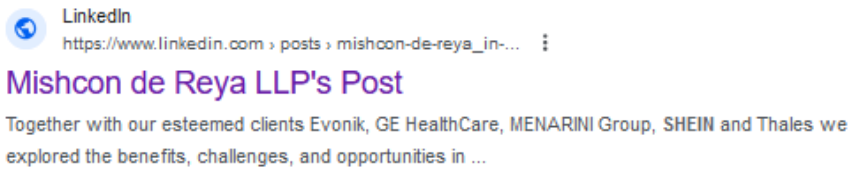
28. According to Mishcon de Reya's website the "*EU Representative service*" furthermore includes:

> "*1. Provide you with a local contact point within the EU/UK. 2. Notify you of any communications from supervisory authorities or data subjects. 3. Keep a copy of your records of data processing activities.*"[16]

29. Additionally, Mishcon de Reya could provide the following services:

> "*1. Liaise with EU/UK supervisory authorities on your behalf. 2. Facilitate effective communication between you and your data subjects, including organising translation services as needed. 3. Provide evidence when required that your business is complying with your representative requirements.*"[17]

30. Therefore, this "*EU Representative service*" does not include making decisions upon the purposes and means of the processing.
31. It is likely that Mishcon de Reya offers this "*EU Representative service*" to SHEIN Singapore as well, since Infinite Styles Ecommerce Co. Limited is registered on the same address as Mishcon de Reya and on LinkedIn Mishcon de Reya also mentions SHEIN as a "*client*":



32. To the extent that an actual office of SHEIN at Infinite Styles Ecommerce Co. Limited is registered at 1-2 Victoria Buildings, Haddington Road, Dublin 4, it is clear that the people who claim to work there, are – based on their LinkedIn profiles – not authorised to decide on the purposes and means of the processing.

[15] https://www.mishcon.com/products/assign
[16] https://www.mishcon.com/products/assign
[17] https://www.mishcon.com/products/assign

33. Based on SHEIN's annual turnover, there is also no way that these 30 employees that are employed by Infinite Styles Ecommerce Co. Limited are making the decisions on the means and purposes of data processing.
34. Because of this, it is extremely unlikely that this address in Dublin is anything more than just a "letterbox" address. Therefore, this Complaint is directed against SHEIN Singapore, since the "letterbox" address in Ireland cannot be considered a main establishment in the EU under Article 4(16)(a) GDPR, which decides on the purposes and means and has the power to implement decisions, since the "*EU Representative service*" does not include making such decisions.[18]
35. This is also confirmed by the EDPB's recent Opinion 04/2024, where is stated:

> "[…] *a controller's PoCA ["place of central administration"] in the Union can be considered as a main establishment under Article 4(16)(a) GDPR only if it takes the decisions on the purposes and means of the processing of personal data and it had power to have these decisions implemented."*[19]

36. Since the foregoing shows that there is no evidence that the place of central administration in the EU, Infinite Styles Ecommerce Co. Limited in Ireland, takes the actual decision on the purposes and means of the processing, nor evidence that it has the power to have such decisions implemented, this means that:

> "[…] *there is no main establishment under Article 4(16)(a) GDPR for that processing. Therefore, in that case, the one-stop-shop mechanism does not apply."*[20]

37. Therefore, the Garante per la protezione dei dati personali (hereinafter: "*Garante*") is the competent authority to handle this Complaint, since the habitual residence of the Complainant is [redacted] and the place of the alleged infringements is also [redacted] (Article 77(1) GDPR). Because of this, the Garante is the competent to exercise the powers in accordance with the GDPR on the territory of Italy (Article 55(1) GDPR).

4. VIOLATIONS OF THE GDPR

4.1. Violation of Chapter V GDPR

38. As described in paragraph 2.3 of this Complaint, SHEIN's Privacy Policy shows that the personal data of the Complainant is in fact being transferred to China (**Annex 3**, e.g. Section 9).
39. 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

[18] EDPB Opinion 2024/04, para. 32; cf. Recital 36 GDPR.
[19] EDPB Opinion 2024/04, para. 27.
[20] EDPB, Opinion 2024/04, para. 29-30.

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)

40. The EU Commission has not decided that China ensures an adequate level of protection (cf. Article 45(1) GDPR). Therefore, SHEIN cannot transfer personal data of the Complainant to China on the basis of an adequacy decision.
41. Because of this, according to its Privacy Policy, SHEIN transfers personal data on the basis of appropriate safeguards (Article 46 GDPR), such as the EU Commission's standard contractual clauses (hereinafter: "*SCCs*") (Article 46(2)(c) GDPR), or on the basis of Article 49(1)(b) GDPR (**Annex 3**, Section 9).
42. 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 appropriate safeguards under Article 46 GDPR.[21]
43. Only in the absence of mechanisms under Article 45 and Article 46 GDPR, derogations provided in Article 49(1) GDPR can be used.[22] Since the derogation of Article 49(1)(b) GDPR can only be used where the transfer is occasional and necessary in relation to the contract (Recital 111 GDPR), it is unlikely this transfer mechanism can be used by SHEIN.[23] Especially since these derogations have to be interpreted restrictively.[24]

4.1.2 Chinese law impinges the effectiveness of appropriate safeguards

4.1.2.1 "Essentially equivalent level of data protection" requirement

44. 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.*"
45. 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]

[21] 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*".

[22] EDPB Guidelines 2018/02, p. 4.

[23] EDPB Guidelines 2018/02, Section 2.2.

[24] EDPB Guidelines 2018/02, p. 4, see also CJEU C-73/07 (*Satamedia*), para. 56; CJEU C-92/09 and C-93/09 (*Schecke and Eifert*), para. 77; CJEU C-363/14 (*Schrems*), para. 92; CJEU C-203/15 (*Tele2 Sverige*), para. 96.

[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*

46. 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:

    (1) Provide data subjects (the Complainant) with enforceable data protection rights;
    (2) Provide data subjects (the Complainant) with effective legal remedies;
    (3) 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

47. According to SHEIN, the basis of the transfer of personal data of the Complainant to China are appropriate safeguards, such as SCCs (**Annex 3**, Section 9).[28] We would like to note that, in principle, the SCCs and other appropriate safeguards under Article 46 GDPR, only cover commercial data transfers, i.e. date transfers related to the purchases concluded via the Platform.
48. Because of their nature, appropriate safeguards, such as 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

49. Some commentators mention the close alignment of Chinese data protection law (in general) with the European or American data protection law.[29] In reality, however, the Chinese Cybersecurity Law (hereinafter: "*CSL*"),[30] the Chinese

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.).

[28] SHEIN also refers to Article 49(1)(b) GDPR as a transfer mechanism, but as already stated, Since the derogation of Article 49(1)(b) GDPR can only be used where the transfer is occasional and necessary in relation to the contract (Recital 111 GDPR), it is unlikely this transfer mechanism can be used by SHEIN.

[29] 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.

[30] 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

Personal Information Protection Law (hereinafter: "*PIPL*"),[31] the Chinese Civil Code,[32] and the Chinese Data Security Law (hereinafter: "*DSL*")[33] differ substantially from European laws.[34]

50. First, Chinese data localisation laws make it obligatory to store data that was "*collected and produced*" and "*collected and generated*" in China within Chinese territory.[35] Therefore, all data controllers[36] running their business activity (partially) in China – like companies within the SHEIN Group – fall under the duty to store data created in China locally.[37] Because of this, practically any transfer of personal data from Chinese territory abroad (to the EU/EEA) requires prior

---

July 2016, came into force on 1 June 2017).

[31] 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).

[32] 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);

[33] 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).

[34] 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.

[35] **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]

[36] 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*

authorization under the Cyberspace Administration of China Data Transfer Guidelines.[38]

51. 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.[39] As a result, data subjects' access requests and data portability rights become illusionary because these rights are subject to "discretional approval".
52. Second, there is a very high risk that Chinese authorities will request and obtain (unlimited) access to personal data processed by Chinese companies.[40] 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.[41] 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.[42]

---

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].

[37] 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.

[38] 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/

[39] 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.

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

[41] 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.

[42] 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.

53. Chinese laws, such as the National Security Law (hereinafter: "*NSL*"),[43] and the National Intelligence Law (hereinafter: "*NIL*")[44] but also the DSL,[45] are treated as a general legal basis for Chinese authorities' to obtain access to any personal data.[46] 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:

    (1) 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*."[47] 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.[48] (emphasis added)

    (2) 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*".[49] (emphasis added)

54. 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

[43] 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).

[44] 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).

[45] Article 35 DSL.

[46] 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.

[47] [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].

[48] See by analogy with the US Cloud Act: https://www.justice.gov/criminal/cloud-act-resources

[49] 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.

are no effective remedies available to the Complainant (or other EU data subjects).[50]

55. The Transparency Reports of Xiaomi (**Annex 6**; **Annex 7**; **Annex 8** and **Annex 9**) 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:

    (1) 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.

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

56. Although the Respondent and/or SHEIN Group have not published any reports on Chinese authorities' data requests, Xiaomi reports provide solid 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

57. It is almost impossible for a foreign data subject to exercise his/her rights under the PIPL[51] or the Chinese Civil Code.[52]
58. First, there is no dedicated, independent and competent data protection authority in China.[53] The CAC plays an important role in Chinese data protection law,[54]

---

[50] WP29 Adequacy Referential, WP254/01 (endorsed by the EDPB: link, under 15), p. 9.

[51] 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).

[52] 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.

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

[54] 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.

although for some provisions it is very difficult to indicate which authority is actually responsible for a particular task.[55] It is worth emphasising that the CAC is closely related to the State Council,[56] and as such may pursue political goals rather than effective independent supervision of data processing activities.

59. 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[57] and the 132nd position in category of restraints imposed by the courts on government powers.[58] 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.[59] This impossibility extends to obtaining effective administrative or judicial redress or claiming compensation as a data subject under the PIPL or the Chinese Civil Code.[60]
60. Third, when Chinese law enforcement or national security authorities request access to personal data, these Chinese authorities follow the "black box" route,[61] making it impossible for a data subject, to understand how exactly such requests have been or will be granted.[62] This makes it impossible to exercise any data protection rights in this regard.

---

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

[56] 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.

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

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

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

[60] 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

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

[62] 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.

61. 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.[63] 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.[64]

4.1.3 Conclusion: SHEIN violates Chapter V GDPR

62. 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 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.[65]
63. Article 44 GDPR requires SHEIN 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.[66] 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.[67]

5. APPLICATIONS

64. 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 Garante 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

[63] P. Cai, L. Chen, 'Demystifying Data Law in China: A Unified Regime of Tomorrow', *International Data Privacy Law* 2022/5, p. 79.
[64] 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.
[65] Cf. EDPB Recommendations 01/2020, para 72.
[66] CJEU C-311/18 (*Schrems II*), para. 101-104.
[67] EDPB Recommendations 01/2020, para 75.

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

65. 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 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."*

66. 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."*

67. 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.* [...]"

68. 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 Garante has a duty to act in this case.

5.2. Investigation under Article 58(1) GDPR

69. Given that some of the details of the processing of the Complainant's personal data by SHEIN are unclear, we hereby request a full investigation of the Garante 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 the Respondent and SHEIN Group, (and therefore the roles of the parties), in particular with regard to the processing of the Complainant's personal data by SHEIN Group.
- Obtaining the "Transfer Impact Assessment", or any documents or communications relating thereto, that the Respondent should have conducted pursuant to Article 46(1) GDPR, including any supplementary measures taken by the Respondent.
- Obtaining the record of processing activities under Article 30 GDPR.

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

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

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

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

71. Additionally, the Complainant also requests the Garante to state:

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

(2) That the transfers of the Complainant's personal data to third countries by the Respondent are unlawful.

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

72. It is our view that that the Respondent 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.
73. Therefore, we suggest that the Garante to impose a fine on the Respondent in accordance with Article 58(2)(i) GDPR. We note that Article 83(1) GDPR requires the Garante to impose fines that are "*effective, proportionate and dissuasive*".

6. CONTACT

74. Communications between *noyb* and the Garante in the course of this procedure can be done by email at [redacted] with reference to the **Case-No C093-02** or [redacted].