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

Hellenic Data Protection Authority
Kifisias 1-3,
Athens, 11523
Greece

Via the Online Services of the HDPA

Vienna, 16 January 2024

noyb Case-No: **C093-06**

Complainant: [redacted]

Xiaomi account 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: **Xiaomi Singapore Pte. Ltd.**
20 China Court Cross Street 02-12
Singapore 048422

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 172/4/3/2, 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 ("*Xiaomi*")

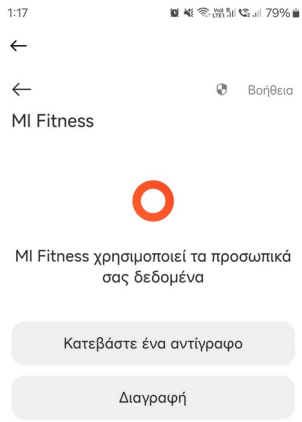
3. Xiaomi Singapore Pte. Ltd. (hereinafter: the "*Respondent*" or "*Xiaomi*") is a multinational "*consumer electronics and smart manufacturing company*", according to its website.[1] More specifically, the Respondent provides users with a variety of IT products and services, including mobile phones, laptops and many other smart devices. Xiaomi is a part of Xiaomi Group, with Xiaomi Inc. being the mother company.[2]
4. Redmi Watch 2 Lite (hereinafter: the "watch") with its accompanying Fitness Application, called "*Mi Fitness*" (hereinafter: the "Mi Fitness") is one of the products that Xiaomi has released to the public as part of its wearable band series.[3] Mi Fitness allows the user to track their use of the watch and to synchronize their fitness data from their device. Fitness data tracked and synced with Mi Fitness includes, among others, steps taken during exercise, number of calories burned, heart rate and sleep data. Mi Fitness provides guidance on workouts and fitness goals to the users, aiming to substitute a personal trainer.

2.2. Complainant

5. The complainant is the owner of a Redmi Watch 2 Lite. She has synced the data from her watch on the Mi Fitness app on her smartphone, since the fall of 2023. For this reason, she has created a Xiaomi account with unique number [redacted].
6. According to the MiFitness' Privacy Policy, MiFitness collects and presents "*training and health information*", such as the information mentioned in para. 4 above (**Annex 3,** under "*Introduction*").
7. 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 the Respondent. For that purpose, the MiFitness app directed her

[1] See here: https://www.mi.com/global/about/
[2] See here: https://ir.mi.com/corporate-information/corporate-governance
[3] See here: https://www.mi.com/global/product/redmi-watch-2-lite/

to her personal account settings, where she could download a copy of her personal data (**Screenshot 1**).



Screenshot 1. The "download your data" function within the Mi Fitness app

8. After downloading the file, it turned out that the Respondent provided the Complainant only with a raw copy of her personal data in an unstructured form in several different folders (**Annex 4**). Thus, it was not feasible for the Complainant to read and understand the information provided by the Respondent.
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 (**Annex 4**), she decided to file an access request under Article 15 GDPR on [redacted] 2024 (**Annex 5**). The access request was sent to the Xiaomi Privacy Team through the Xiaomi Privacy Requests form (**Annex 5**), the link to which is provided in the respondent's Privacy Policy (**Annex 3**, under "*5.2. Your rights with regard to your personal information*").
10. The Respondent never acted on the Complainant's access request. The complainant has not received a reply to her request since the day of its submission.

2.3. Xiaomi's company structure

11. In its 2023 Annual Report, Xiaomi Inc. lists its subsidiaries/controlled structured entities.[4] Xiaomi Singapore Pte. Ltd. is included in this list as an entity established in December 23, 2013.
12. Xiaomi Inc. is a joint-stock company registered in Beijing (China) and listed on the Hong Kong Stock Exchange. Xiaomi Inc. plays a crucial role in the structure of the Xiaomi Group. It is worth noting that subsidiaries of Xiaomi Inc., including Xiaomi Singapore, are responsible for a significant amount of the Xiaomi Group revenue. In its 2023 Annual Report, Xiaomi Inc. lists its subsidiaries/controlled structured entities. It is, therefore, a relatively new company that is directly owned by Xiaomi Inc. at a percentage of 100%.[5] It follows that Xiaomi Inc. has final say and the control over the means and the purpose of the processing of the data subjects personal data as they control 100% of the resources of Xiaomi Singapore.
13. Additionally, in order to effectively manage the Xiaomi Group, decisions regarding key aspects of its activity are made at the highest level of the structure within the Xiaomi Inc., in Beijing (**Screenshot 2**):

Xiaomi Corporation ('Xiaomi' or the 'Company', together with its subsidiaries and companies consolidated for accounting purposes, the 'Group') is an internet company with smartphones and smart hardware connected by an IoT platform at its core. The shares in the Company are listed on the Main Board of the Stock Exchange of Hong Kong. The directors of Xiaomi recognise the need to conduct the business of the Group with integrity and in accordance with suitable governance practices. The requisite improvements to the Group's corporate governance procedures and policies have either been implemented or are in the process of being made.

	Audit Committee	Remuneration Committee	Nomination Committee	Corporate Governance Committee
Lei Jun ★		👤		
Lin Bin ☆			👤	
Liu Qin	👤			
Chen Dongsheng	👤	👤		👤
Wong Shun Tak	👤	👤	👤	👤
Cai Jinqing			👤	👤

👤 = Chairperson 👤 = Member ★ = Chairman of the Board ☆ = Vice-Chair of the Board

Screenshot 2. Committees of Xiaomi Group

---

14. According to the Xiaomi Group ESG Report 2023, Xiaomi pays special attention to data protection and cybersecurity. Therefore, the company has appointed an

[4]Xiaomi Corporations, 2023 Annual Report, p. 272, 274, https://ir.mi.com/system/files-encrypted/nasdaq_kms/assets/2024/04/25/5-36-08/2023%20Annual%20Report.pdf

[5] Xiaomi Corporation, 2023 Annual Report, p. 272, https://ir.mi.com/system/files-encrypted/nasdaq_kms/assets/2024/04/25/5-36-08/2023%20Annual%20Report.pdf

'Information Security and Privacy Committee' within its Xiaomi Inc. entity, as follows:

> *"At Xiaomi, we actively foster an internal culture of privacy and have established a privacy management system comprised of organizations, policies, and procedures. We have appointed a Chief Privacy Officer and formed an Information Security and Privacy Committee covering all business teams to better coordinate and advance our privacy protection efforts throughout the Group. Additionally, we collaborate with users, privacy experts, and third-party certification agencies to continuously improve our privacy practices at Xiaomi."*
>
> *The Group has established an Information Security and Privacy Committee (the "Security Privacy Committee"), which focuses on developing and implementing rules, managing security risks associated with personal privacy, advancing privacy technology capabilities, and enhancing risk response abilities. This year, we completed the change of term and reorganization of the Security Privacy Committee. Each business department now operates a Security and Privacy Working Group, contributing to a more mature data security system for the Group and effectively empowers the secure development of smartphones and other business lines. Xiaomi's Board places great importance on data security and privacy protection. The Security Privacy Committee reports to the Board periodically on the Group's progress in this area and assists the Board in assessing risks in data security and privacy protection, countermeasures, and their efficacy."*

2.4. Xiaomi's Privacy Policy for MiFitness

15. Since the Complainant's habitual residence is located within the EU/EEA, and specifically in Greece, Xiaomi's Privacy Policy for MiFitness for Greek users applies, which is also accessible in Greek (**Annex 3**).[6] The complainant used the "*Download a copy* [of your data]" feature to obtain access to her personal data and to check whether there were data transfers to third countries, including China, (**Screenshot 1**).
16. The Respondent claims its Privacy Policy covers the processing activity regarding data related to the Platform the Complainant is using (**Annex 3,** "*Introduction*").
17. The section "*3. How your personal information is transferred globally*" of the Respondent's Privacy Policy describes Xiaomi's international data transfers. Xiaomi mentions that it "*operates facilities around the world that process and back up personal information.*" According to the Privacy Policy, any personal data of the Complainant may be transferred to a number of third countries, including to China.[7] (**Annex 3**, under 3.).

[6] For the current available version of the MiFitness Privacy Policy, see here: https://watch.xiaomiwear.com/html/privacy/index.html?type=sport_healthy_privacy&model=app&locale=el

[7] *"Currently, Xiaomi has data centers in **China**, **India, the United States, Germany, Russia, and Singapore.** As per this Privacy Policy, **your information may be transferred to these data centers in***

18. That the Complainant's personal data is being transferred to China, as well as other countries, is acknowledged by the fact that the section "*How your personal information is transferred globally*" (Section 3) of Xiaomi's Privacy Policy states:

> "*We may also share your personal information with our third-party service providers and business partners, and as a result, your information may also be transferred to other countries. In these jurisdictions, standards of personal information protection might be different from the standards applied in your jurisdiction. There may be risks under different data protection laws. However, this does not change our commitment to comply with this Privacy Policy and protect your personal information.*[…]." (**Annex 3**, under 3.).

19. Furthermore, Xiaomi's Privacy Policy describes Xiaomi "*may publicly disclose your personal information under the following circumstances:*" (**Annex 3**, Section 2.3. under "*Public Disclosure*"):

> "*Public disclosure based on law or reasonable grounds, including laws and regulations, legal procedures, litigation, or at the request of relevant government departments.*" (**Annex 3**, under Section 2.3.)

Since these public disclosures based on "*law or reasonable grounds, including laws and regulations, legal procedures, litigations*" and "*at the request of relevant government departments*" are not limited to requests under EU-law, these also include "*public disclosures*" under Chinese (intelligence service) laws.

20. The Respondent states in its Privacy Policy that if *"Xiaomi transfers your data generated in the European Economic Area (EEA) to Xiaomi's affiliated organizations or third-party services provided outside the EEA, we will do so in accordance with the security mechanisms provided in the EU Standard Contractual Clauses or the General Data Protection Regulation (GDPR)*." (**Annex 3**, Section 3, under "*How your personal information is transferred globally*").

2.5. Chinese government access to Xiaomi's user data

21. Xiaomi Inc., confirmed that they receive many requests from various Chinese public authorities regarding user data.[8] 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**).
22. Chinese law grants the authorities with unrestricted powers regarding access to data processed by, inter alia, Chinese companies.[9] Thus, it is very likely that the

accordance with applicable laws." (**Annex 3,** under 3.).

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

[9] 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:

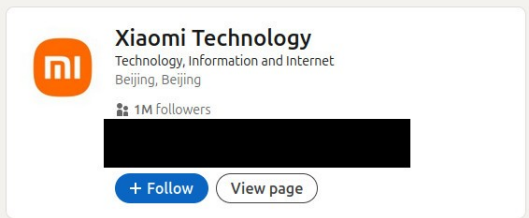
Respondent, being a subsidiary of a Chinese company and part of the Xiaomi Group, also receives a very high number of requests by Chinese government bodies and has to give access to personal data in case of such requests, since the same laws apply to them.

2.6. Second complaint

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

3. COMPETENT AUTHORITY

24. Xiaomi claims that for all data processing of EU customers, Xiaomi Technology Netherlands Ltd. in the Netherlands is the data controller and Xiaomi Singapore Pte Ltd "*will be responsible for data processing*" (**Annex 3**, Section 3, under "*How your personal information is transferred globally*").
25. It is obvious from this ambiguous wording by the Respondent that Xiaomi Technology Netherlands does not determine the means and the purpose of processing. On the contrary, Xiaomi Singapore Pte Ltd is the one determining the means and the purposes of the data processing at hand, since the Respondent establishes in writing that the Singaporean entity is the one who conducts all the data processing.
26. It is hard to believe that The World Trade Center building in Pr. Beatrixlaan 582 Str., 2595 BM in the Hague in the Netherlands is the Respondent's actual main establishment, especially since even a small search on the LinkedIn company's page shows Xiaomi Technology being based in Beijing, China (**Screenshot 3**), and only 7(!) people working for the Respondent in the Hague.[10]



Screenshot 3. Xiaomi Technology's LinkedIn page

2017); EDPS Government access to data in third countries, EDPS/2019/02-13, link.

[10] For the exact search results see here: https://www.linkedin.com/search/results/people/?currentCompany=%5B%222300557%22%5D&geoUrn=%5B%22102685993%22%5D&keywords=Xiaomi&origin=FACETED_SEARCH&sid=imD

27. To the extent there is an actual office of Xiaomi at Pr. Beatrixlaan 582 Str., 2595 BM in the Hague, 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[11].
28. Because of this, it is extremely unlikely that this address in the Hague is anything more than just a "letterbox" address. Therefore, this Complaint is directed against Xiaomi Singapore Pte Ltd., since the "letterbox" address in the Netherlands cannot be considered a main establishment in the EU under Article 4(16)(a) GDPR, which decides on the purposes and means (of processing) and has the power to implement decisions, since even the Respondent explicitly states so in their Privacy Policy.
29. 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."*[12]

30. The foregoing shows that there is no evidence that the place of central administration in the EU, Xiaomi Netherlands B.V., in the Hague, 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."*[13]

31. Therefore, the Hellenic Data Protection Authority (hereinafter: "*HDPA*") 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 HDPA is the competent to exercise the powers in accordance with the GDPR on the territory of Greece (Article 55(1) GDPR).

4. VIOLATIONS OF THE GDPR

4.1. Violation of Chapter V GDPR

32. As described in paragraph 2.3 of this Complaint, the Respondent's Privacy Policy shows that the personal data of the Complainant is in fact being transferred to China (**Annex 3**, e.g. Section 3).
33. 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

[11] See previous footnote.
[12] EDPB Opinion 2024/04, para. 27.
[13] EDPB, Opinion 2024/04, para. 29-30.

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)

34. The EU Commission has not decided that China ensures an adequate level of protection (cf. Article 45(1) GDPR). Therefore, Xiaomi cannot transfer personal data of the Complainant to China on the basis of an adequacy decision.
35. Because of this, according to its Privacy Policy, Xiaomi 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).
36. 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.[14]
37. Only in the absence of mechanisms under Article 45 and Article 46 GDPR, derogations provided in Article 49(1) GDPR can be used.[15] 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 Xiaomi.[16] Especially since these derogations have to be interpreted restrictively.[17]

4.1.2 Chinese law impinges the effectiveness of appropriate safeguards

4.1.2.1 "Essentially equivalent level of data protection" requirement

38. 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.*"
39. 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.[18] Nevertheless, the controller who relies upon appropriate safeguards under Article 46 GDPR – such as SCCs – also needs to verify to what extent the

[14] 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*".
[15] EDPB Guidelines 2018/02, p. 4.
[16] EDPB Guidelines 2018/02, Section 2.2.
[17] 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.
[18] CJEU C-363/14 (*Schrems I*), CJEU C-293/12 and C-594/12 - Digital Rights Ireland.

third country law satisfies a data protection level equivalent to the EU level of data protection.[19]

40. 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.[20]

4.1.2.2 Violation of Article 7 and 8 CFR

(A) Commercial data transfers

41. According to the Respondent, the basis of the transfer of personal data of the Complainant to China are appropriate safeguards, such as SCCs (**Annex 3**, Section 3). 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.
42. 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

43. Some commentators mention the close alignment of Chinese data protection law (in general) with the European or American data protection law.[21] In reality, however, the Chinese Cybersecurity Law (hereinafter: "*CSL*"),[22] the Chinese

[19] 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*."

[20] CJEU C-311/18 (*Schrems II*), para 103-105; WP29 Adequacy Referential, WP254rev.01, Chapter 4 (endorsed by the EDPB: link , under 15.).

[21] 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.

[22] 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*"),[23] the Chinese Civil Code,[24] and the Chinese Data Security Law (hereinafter: "*DSL*")[25] differ substantially from European laws.[26]

44. 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.[27] Therefore, all data controllers[28] running their business activity (partially) in China – like companies within the Xiaomi Group – fall under the duty to store data created in China locally.[29] 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).

[23] 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).

[24] 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);

[25] 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).

[26] 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.

[27] **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]

[28] 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.[30]

45. 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.[31] As a result, data subjects' access requests and data portability rights become illusionary because these rights are subject to "discretional approval".
46. Second, there is a very high risk that Chinese authorities will request and obtain (unlimited) access to personal data processed by Chinese companies.[32] 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.[33] 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.[34]

---

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].

[29] 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.

[30] 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/

[31] 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.

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

[33] 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.

[34] 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.

47. Chinese laws, such as the National Security Law (hereinafter: "*NSL*"),[35] and the National Intelligence Law (hereinafter: "*NIL*")[36] but also the DSL,[37] are treated as a general legal basis for Chinese authorities' to obtain access to any personal data.[38] 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:

    (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*."[39] 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.[40] (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*".[41] (emphasis added)

48. 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

[35] 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).

[36] 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).

[37] Article 35 DSL.

[38] 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.

[39] [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].

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

[41] 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).[42]

49. 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:

    (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.

4.1.2.3 Violation of Article 47 CFR

50. It is almost impossible for a foreign data subject to exercise his/her rights under the PIPL[43] or the Chinese Civil Code.[44]

51. First, there is no dedicated, independent and competent data protection authority in China.[45] The CAC plays an important role in Chinese data protection law,[46] although for some provisions it is very difficult to indicate which authority is actually responsible for a particular task.[47] It is worth emphasising that the CAC is

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

[43] 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).

[44] 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.

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

[46] 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.

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

closely related to the State Council,[48] and as such may pursue political goals rather than effective independent supervision of data processing activities.

52. 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[49] and the 132nd position in category of restraints imposed by the courts on government powers.[50] 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.[51] 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.[52]
53. Third, when Chinese law enforcement or national security authorities request access to personal data, these Chinese authorities follow the "black box" route,[53] making it impossible for a data subject, to understand how exactly such requests have been or will be granted.[54] This makes it impossible to exercise any data protection rights in this regard.
54. 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

[48] 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.

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

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

[51] 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

[52] 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

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

[54] 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.

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.[55] 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.[56]

4.1.3 Conclusion: Xiaomi violates Chapter V GDPR

55. 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.[57]
56. Article 44 GDPR requires Xiaomi 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.[58] 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.[59]

5. APPLICATIONS

57. 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 HDPA 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.

[55] P. Cai, L. Chen, 'Demystifying Data Law in China: A Unified Regime of Tomorrow', *International Data Privacy Law* 2022/5, p. 79.
[56] 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.
[57] Cf. EDPB Recommendations 01/2020, para 72.
[58] CJEU C-311/18 (*Schrems II*), para. 101-104.
[59] EDPB Recommendations 01/2020, para 75.

- *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

58. 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."*

59. 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."*

60. 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.* [...]"

61. 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 HDPA has a duty to act in this case.

5.2. Investigation under Article 58(1) GDPR

62. Given that some of the details of the processing of the Complainant's personal data by Xiaomi 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 Xiaomi Group, (and therefore the roles of the parties), in particular with regard to the processing of the Complainant's personal data by Xiaomi 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

63. Even before any investigation may have come to a final conclusion, we urge the HDPA to already take imminent, preliminary steps to ensure that the Respondent 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 Xiaomi services' users to China, under Article 58(2)(j) GDPR;

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

64. Additionally, the Complainant also requests the HDPA to state:

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

(b) 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

65. 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.

66. Therefore, we suggest that the HDPA 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

67. Communications between *noyb* and the HDPA in the course of this procedure can be done by email at [redacted] with reference to the **Case-No C093-06** or [redacted].