



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

Hellenic Data Protection Authority  
Kifissias 1-3  
11523 Athens, GREECE

Via the HDPA's online services

Vienna, 16 January 2024

**noyb Case-No: C093-04**

Complainant:

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

TikTok username: [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:

**ByteDance Ltd.,**  
P.O. Box 31119 Grand Pavilion,  
Hibiscus Way, 802 West Bay Road,  
Grand Cayman, KY1 - 1205 Cayman Islands.

And alternatively:

**TikTok Technology Limited,**  
The Sorting Office, Ropemaker Place,  
Dublin 2, Dublin, D02 HD23, Ireland.

**TikTok Inc.,**  
5800 Bristol Parkway, Suite 100,  
Culver City, CA 90230, United States of America

**TikTok Pte. Ltd.,**  
Raffles Quay, #26-10, South Tower,  
Singapore 048583, Singapore<sup>1</sup>

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**

---

<sup>1</sup> After investigation of the relationship among the companies that belong to the ByteDance group, it became clear that the respondent for this complaint cannot be TikTok Technology Limited company, established in Ireland, as the resources that are related to the processing of personal data are controlled by the ByteDance mother company and the data transfers take place among multiple entities within the group. In this case the controller is according to our findings ByteDance, Ltd. However, because of the complex structure of the group of companies, this Complaint is addressed to all entities that are thought to play at least a role in the processing under investigation.

## 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 (“ByteDance”)

3. The Respondent is the mother company behind TikTok, “*the leading destination for short-form mobile video*” (hereinafter: “*Platform*”), according to the Platform’s website.<sup>2</sup> More specifically, TikTok is a social media platform on which users can interact with each other through the above mentioned short-form videos<sup>3</sup>. According to Google’s data on Google Play, the TikTok app for Android smartphones has been downloaded more than a billion times.<sup>4</sup>
4. The Respondent was founded in 2012 in China, with a registered seat in the Cayman Islands<sup>5</sup>. TikTok was launched in 2016<sup>6</sup>. Even though TikTok’s headquarters are in Los Angeles and Singapore, it operates offices in multiple locations worldwide and, specifically, in New York, London, Dublin, Paris, Berlin, Dubai, Jakarta, Seoul, and Tokyo.<sup>7</sup> TikTok’s counterpart in China is Douyin<sup>8</sup>, whose logo even includes TikTok’s logo (**Screenshot 1**).



Screenshot 1. Douyin’s logo.

---

5. Douyin Group Ltd., the company behind the Douyin platform, one of multiple subsidiaries of ByteDance, is located in Hong Kong and all of its subsidiaries are based in China as seen in the Group’s Corporate Structure (**Screenshot 2**).

---

<sup>2</sup> “TikTok is the leading destination for short-form mobile video. Our mission is to inspire creativity and bring joy.” <https://www.tiktok.com/about?lang=%7Blang%7D>

<sup>3</sup> “Today, the TikTok platform, which is available outside of China, has become the leading destination for short-form mobile videos worldwide.” See here: <https://www.bytedance.com/en/>

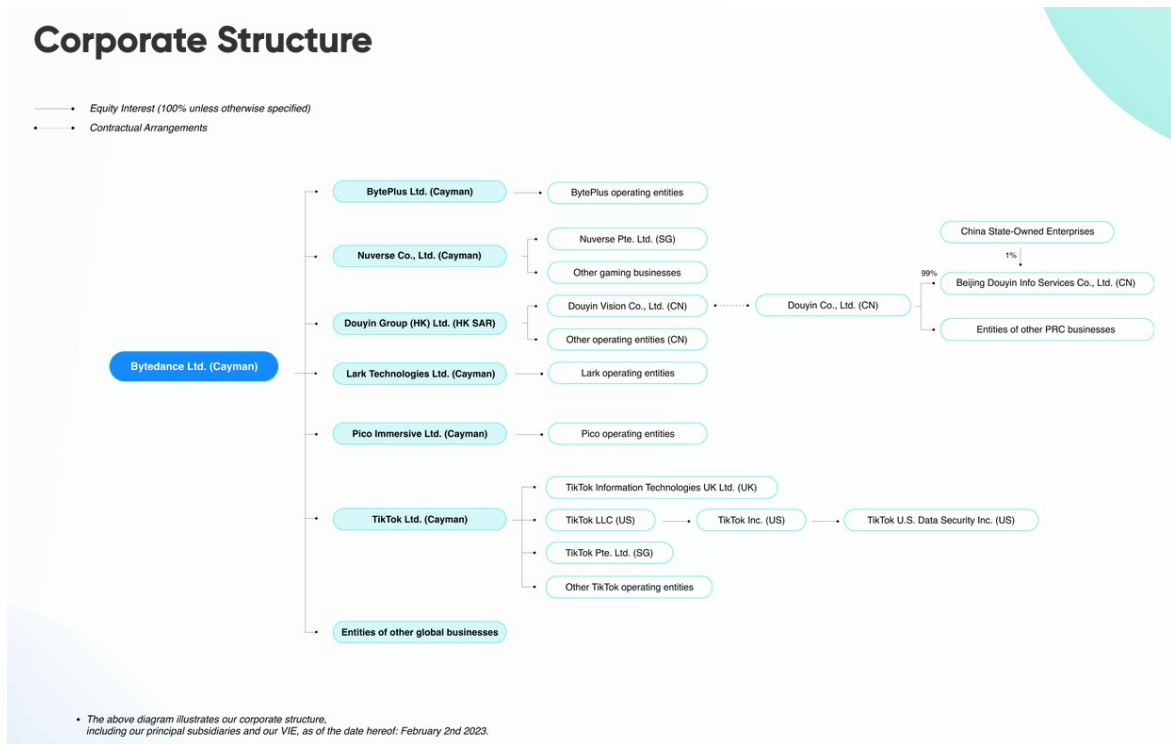
<sup>4</sup> See here: <https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically&hl=en&pli=1>

<sup>5</sup> See here: <https://digiday.com/media/everything-you-need-to-know-about-bytedance-the-company-behind-tiktok/> and <https://www.bytedance.com/en/>

<sup>6</sup> See here: <https://www.investopedia.com/what-is-tiktok-4588933>

<sup>7</sup> See here: <https://www.tiktok.com/about?lang=en>

<sup>8</sup> See here: <https://www.douyin.com/>



*Screenshot 2. ByteDance’s Corporate Structure.*

6. 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**, as downloaded from the Internet Archive snapshot of the webpage<sup>9</sup>, under “*EEA/UK/CH*”).<sup>10</sup>
7. Despite its multiple locations and its efforts to alienate itself from ByteDance, TikTok remains heavily influenced by its China-based mother company, according to several news reports<sup>11</sup>. This influence is proven by the fact that employees where working with ByteDance managers, despite having been assigned new

<sup>9</sup>For the original page, see here: <https://web.archive.org/web/20240813125023/https://www.tiktok.com/legal/page/eea/privacy-policy/en>

<sup>10</sup> **Annex 3**, e.g. “*EEA/UK/CH*”: “If you live in the European Economic Area, United Kingdom, or Switzerland, this Privacy Policy will apply.”

<sup>11</sup>See here: <https://archive.ph/20240415152320/https://fortune.com/2024/04/15/tiktok-china-data-sharing-bytedance-project-texas/#selection-1084.0-1084.1> , <https://restofworld.org/2024/tiktok-chinese-us-ban/> , <https://www.forbes.com/sites/emilybaker-white/2022/09/21/tiktok-bleeding-us-execs-china-control-bytedance/?sh=65bea6f19707> , <https://gizmodo.com/tiktok-master-messaging-pr-playbook-china-music-1849334736>

(American) ones.<sup>12</sup> In addition, according to these reports, American employees would still send copies of spreadsheets filled with user data to ByteDance employees in Beijing well after the two companies had supposedly separated their ways.<sup>13</sup>

8. ByteDance claims that for all data processing of EEA/EU customers, TikTok Technology Limited in Ireland and TikTok Information Technologies UK Limited in the UK are the joint controllers of the users' personal data (**Annex 3**, "Introduction") (see also paragraph 3 of this Complaint).

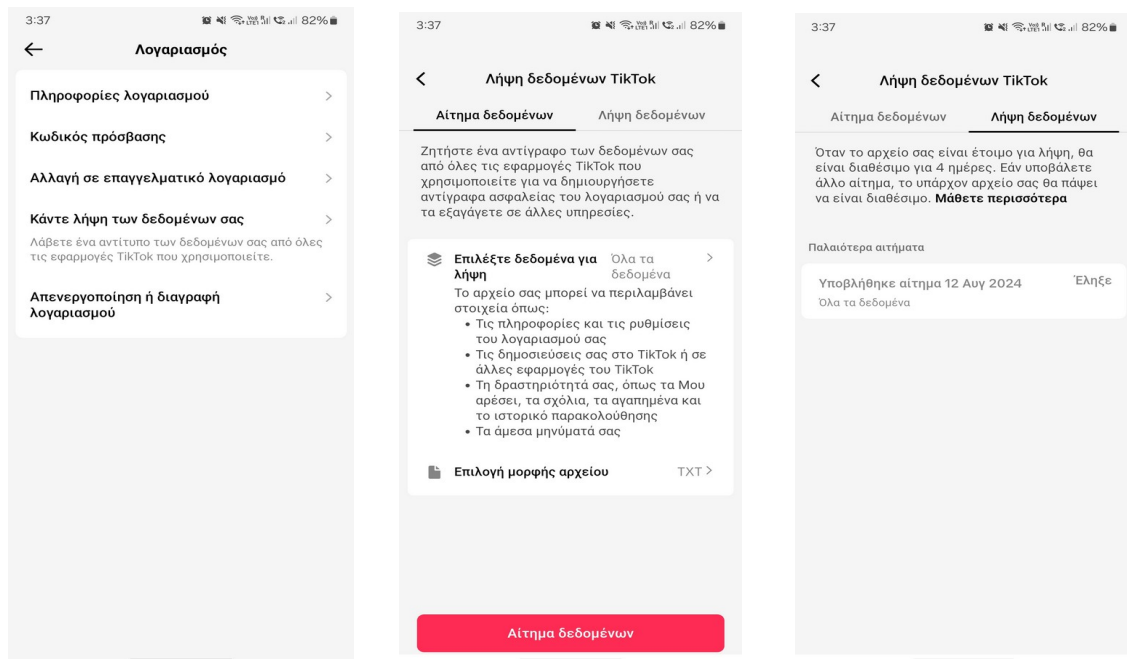
## 2.2. Complainant

9. The Complainant is a user of the Platform [REDACTED]. To use the Platform and to be able to interact on it, the Complainant had to create an account and provide her personal data. According to the Platform's Privacy Policy, TikTok collects and processes personal data, such as identity and contact information (such as an e-mail address, name, username), profile data (such as interests), user content, messages and contacts and other connections among others (**Annex 3**, under "What Information We Collect").
10. On [REDACTED] 2024, the Complainant tried to access her personal data, to verify whether her personal data was being transferred to China or any other third country by the Respondent. For that purpose, the TikTok app directed her to her personal account settings, where she could download a copy of her personal data (**Screenshot 3**). After downloading the file, it turned out that the Respondent provided the Complainant only with a limited list of personal data processed by the respondent (**Annex 4**), including her TikTok activity, email address, username, but without it including any information regarding data transfers.

---

<sup>12</sup>See here: <https://archive.ph/20240415152320/https://fortune.com/2024/04/15/tiktok-china-data-sharing-bytedance-project-texas/#selection-1105.248-1105.454>

<sup>13</sup>See here: <https://archive.ph/20240415152320/https://fortune.com/2024/04/15/tiktok-china-data-sharing-bytedance-project-texas/#selection-1105.248-1105.454>



*Screenshot 3. The Complainant received a limited list of personal data after clicking on the “Download your Data” feature on the complainant’s TikTok for Android app.*

11. 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 August 13, 2024. The access request was sent to the TikTok Privacy Team through the TikTok Privacy Requests form (**Screenshot 4**), the link to which is provided in the respondent’s Privacy Policy (**Annex 3**, under “*Contact Us*”).

**Submit a privacy request**

TikTok values your privacy and safety, and we believe in data transparency. This form is intended only for the following purposes. Fill out this form if you would like to:

- Exercise your rights under data protection laws
- Report a potential Privacy Violation

Before you continue, review the following options:

- If you have a request regarding your TikTok account, your content, or our Community Guidelines, please visit our [Help Center](#).
- If you are seeking customer support, please contact our [Safety Support](#) team.
- If you are a prospective employee or a former employee, please submit your privacy concerns using the [TikTok HR Data Subject Request Form](#).

**Your country or region of residence\***  
If your account was registered in the United States, please submit your request using the [US privacy request form](#)

Greece

**Email address\***  
We'll use this email to contact you about the request. If possible, use the email associated with your TikTok account.

email@domain

**Do you have a TikTok account? \***

Yes

**Your TikTok username\***  
Enter your username without the "@" symbol

username

**Submit a request \***

Exercise your rights under data protection laws

**Select a subcategory \***

I want to download my TikTok data

To download your TikTok data:  
Visit the Help Center article: [Requesting your data](#).

If you had issues when downloading your data through our in-app tool, provide details:

Input text

**Declarations**

Confirm these statements are true before you submit.

I ensure, to the best of my ability and knowledge, that all the information disclosed above is accurate and true.

I understand that abuse of the Global Privacy Form may result in account suspension.

**Attachments**

Up to 5 files can be uploaded. Accepted formats: PDF, PNG, JPEG, MP4, and MOV. **Do not upload any personal information.** If we need more information, we will contact you.

Add files

Submit

Visit our [Privacy Policy](#) to learn more about how we collect, use, and share personal information. Our [Community Guidelines](#) also define what types of content are considered privacy violations.

Screenshot 4. The Complainant submitted their access request through the Platform's Privacy Requests form.<sup>14</sup>

12. On ██████████ 2024 the Respondent replied to the access request via email. In this email the Respondent referred the Complainant to the information in its Privacy Policy and to the possibility of downloading a copy of her personal data (which as is stated above, did not provide the Complainant with the information under Article 15(1),(2),(3)) (**Annex 5**).
13. However, none of these responses did include an answer to the Complainant's questions regarding data transfers to China or any other third country by the Respondent.

## 2.3. The Platform's Privacy Policy

14. Since the Complainant's habitual residence is located within the EU/EEA, the Platform's Privacy Policy for European users applies (**Annex 3**).<sup>15</sup> When the

<sup>14</sup>See here: <https://www.tiktok.com/legal/report/privacy/webform/en>

<sup>15</sup> For the original page see here: <https://web.archive.org/web/20240813125023/https://www.tiktok.com/legal/page/eea/privacy-policy/en>

- Complainant sent the access request to the Respondent on [REDACTED] 2024, the version of November 13, 2023 of the Privacy Policy was applicable (**Annex 3**).
15. TikTok claims its Privacy Policy covers the processing activity regarding data related to the Platform the Complainant is using (**Annex 3**, under “*Introduction*”).
  16. The section “*Our Global Operations and Data Transfers*” of the Platform’s Privacy Policy describes the Platform’s international data transfers. TikTok does not specify the exact location of international data transfers. However, it directs the users and, therefore, the complainant, to another page titled “*Our Global Operations and Data Transfers: Storage and Limited Remote Access within our Corporate Group*”<sup>16</sup>. There the complainant can see that any personal data of the complainant may be transferred to outside of the European Union, including to China.
  17. That the Complainant’s personal data is being transferred to China, is acknowledged by the fact that the section “*Limited Remote Access*” of the previous page<sup>17</sup> mentions:

*“Certain entities in our Corporate Group located in countries without an adequacy decision are granted, under standard contractual clauses, limited remote access to information described in “What Information We Collect” to provide important functions. These entities are located in Australia, Brazil, China, Malaysia, Philippines, Singapore, and the United States.”* (**Annex 3A**, under “*Limited Remote Access*”).

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

18. Furthermore, the Platform’s Privacy Policy describes that TikTok complies with: “*with applicable law, legal process or government requests, as consistent with internationally recognised standards.*” (**Annex 3**, under “*How We Share Your Information*” → “*Others*” → “*Legal Obligations and Rights*”). The Platform even has a “*TikTok Law Enforcement Guidelines*” page<sup>18</sup> where it guides law enforcement officials on how to request users’ data. Since these “*government requests*” are not limited to requests under EU-law, these also include requests under Chinese (intelligence service) laws.
19. TikTok states in its Privacy Policy and its “*Our Global Operations and Data Transfers: Storage and Limited Remote Access within our Corporate Group*” page that it transfers personal data outside the European Union, including China. TikTok transfers data to support its global operations (“*to support our global operations*”). According to the previous page, except for the SCCs, TikTok allows “*Limited Remote Access*” to certain entities in its Corporate Group according to:

---

<sup>16</sup>See here: <https://www.tiktok.com/legal/page/eea/transferee-countries/en>

<sup>17</sup>Meaning the page titled “*Our Global Operations and Data Transfers: Storage and Limited Remote Access within our Corporate Group*”.

<sup>18</sup>See here: <https://www.tiktok.com/legal/page/global/law-enforcement/en>



*“Adequacy decisions. Certain entities in our Corporate Group located in Canada, UK, [Israel](#), [Japan](#) and [South Korea](#) are granted limited remote access to information described in “[What Information We Collect](#)” to provide important functions. We rely on the European Commission [adequacy decisions](#) (or equivalent decisions under other laws) to grant these entities remote access”.*

20. It remains unclear from the Privacy Policy and the above mentioned page which are these entities and which data are transferred to them. However, after observing ByteDance’s Corporate Structure, which includes entities in China (“*Douyin Vision Co. Ltd*” & “*Douyin Co. Ltd*”) and the USA (“*TikTok LLC*” & “*TikTok Inc.*”), as well as Singapore (“*TikTok Pte. Ltd.*”) it is obvious that these “*Global Operations*” include entities of the ByteDance Group operating in those countries.

## 2.4. Chinese government access to TikTok’s user data

21. The Respondent does not provide any information regarding Chinese government requests made directly to them or any of their subsidiaries, nor access given to personal data of users by them upon such requests.
22. However, the Chinese company, Xiaomi Inc., confirmed that they receive many requests from various Chinese public authorities regarding user data.<sup>19</sup> 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**).
23. Neither the Respondent, nor its subsidiaries published 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.<sup>20</sup> Thus, it is very likely that the Respondent, being a subsidiary of a Chinese company and part of the ByteDance Group, also receives a very high number of requests by Chinese government bodies and has to give access to personal data in case of such requests, since the same laws apply to them.

## 2.5. Second complaint

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

---

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

<sup>20</sup> 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](#).

### 3. COMPETENT AUTHORITY

25. The Respondent, on its Platform, claims that for all data processing of EU customers, TikTok Technology Limited in Ireland and TikTok Information Technologies UK Limited are the joint controllers of the “*information processed in connection with this Privacy Policy*” (Annex 3, “Introduction”).
26. However, on the address where TikTok was located at the time of the access request (Annex 3, under “Contact Us”) one would not find the Platform’s offices or any of ByteDance’s establishments but Arthur Cox LLP, a “*full spectrum corporate and business law service*”<sup>21</sup>.
27. It is extremely unlikely that this address is anything more than just a “letterbox” address. Meanwhile, as presented in Section 2.1., ByteDance still has strong ties with the Irish and American entities. Therefore, this Complaint is directed against ByteDance, 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 a law firm that represents the Respondent does not make such decisions.<sup>22</sup>
28. 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.”*<sup>23</sup>

29. Since the foregoing shows that there is no evidence that the place of central administration in the EU, Arthur Cox LLP’s offices 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.”*<sup>24</sup>

30. Therefore, the Hellenic Data Protection Authority (hereinafter: “HDP”) is the competent authority to handle this Complaint, since the habitual residence of the Complainant is in Athens, Greece and the place of the alleged infringements is also in Athens, Greece (Article 77(1) GDPR). Because of this, the HDP is the competent authority to exercise the powers in accordance with the GDPR on the territory of Greece (Article 55(1) GDPR).

---

<sup>21</sup>See here: <https://www.arthurcox.com/contact/dublin/>

<sup>22</sup> EDPB Opinion 2024/04, para. 32; cf. Recital 36 GDPR.

<sup>23</sup> EDPB Opinion 2024/04, para. 27.

<sup>24</sup> EDPB, Opinion 2024/04, para. 29-30.

## 4. VIOLATIONS OF THE GDPR

### 4.1. Violation of Chapter V GDPR

31. As described in paragraph 2.3 of this Complaint, the Platform's Privacy Policy shows that the personal data of the Complainant is in fact being transferred to China (**Annex 3**, under "*Our Global Operations and Data Transfers*").
32. According to Article 44 GDPR, any transfer of personal data to a third country is, in principle, forbidden. A transfer may take place only if the conditions laid down in Chapter V are complied with. As explained below, none of these conditions are met, and therefore, the transfer of personal data of the Complainant to China by the Respondent is unlawful because of the following:

#### 4.1.1 No adequacy decision (Article 45 GDPR)

33. The EU Commission has not decided that China ensures an adequate level of protection (cf. Article 45(1) GDPR). Therefore, the Respondent cannot transfer personal data of the Complainant to China on the basis of an adequacy decision.
34. Because of this, according to its Privacy Policy, the Respondent 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) (**Annex 3A**).
35. This means the Respondent has to conduct a data transfer impact assessment (hereinafter: "TIA"), to verify whether Chinese laws or practices impinge on the effectiveness of the appropriate safeguards under Article 46 GDPR.<sup>25</sup>
36. Only in the absence of mechanisms under Article 45 and Article 46 GDPR, derogations provided in Article 49(1) GDPR can be used.<sup>26</sup> 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 TikTok/the ByteDance Group.<sup>27</sup> Especially since these derogations have to be interpreted restrictively.<sup>28</sup>

---

<sup>25</sup> 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*".

<sup>26</sup> EDPB Guidelines 2018/02, p. 4.

<sup>27</sup> EDPB Guidelines 2018/02, Section 2.2.

<sup>28</sup> 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.

## 4.1.2 Chinese law impinges the effectiveness of appropriate safeguards

### 4.1.2.1 “Essentially equivalent level of data protection” requirement

37. 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.*”
38. 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.<sup>29</sup> 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.<sup>30</sup>
39. 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.<sup>31</sup>

### 4.1.2.2 Violation of Article 7 and 8 CFR

#### (A) Commercial data transfers

40. According to the Platform’s Privacy Policy, the basis of the transfer of personal data of the Complainant to China are appropriate safeguards, such as SCCs (**Annex 3A**). 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. data transfers related to the purchases concluded via the Platform.

---

<sup>29</sup> CJEU C-362/14 (*Schrems I*), CJEU C-293/12 and C-594/12 - Digital Rights Ireland.

<sup>30</sup> CJEU C-362/14 (*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.*”

<sup>31</sup> CJEU C-311/18 (*Schrems II*), para 103-105; WP29 Adequacy Referential, WP254rev.01, Chapter 4 (endorsed by the EDPB: [link](#) , under 15.).

41. 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

42. Some commentators mention the close alignment of Chinese data protection law (in general) with the European or American data protection law.<sup>32</sup> In reality, however, the Chinese Cybersecurity Law (hereinafter: “CSL”),<sup>33</sup> the Chinese Personal Information Protection Law (hereinafter: “PIPL”),<sup>34</sup> the Chinese Civil Code,<sup>35</sup> and the Chinese Data Security Law (hereinafter: “DSL”)<sup>36</sup> differ substantially from European laws.<sup>37</sup>
43. First, Chinese data localisation laws make it obligatory to store data that was “collected and produced” and “collected and generated” in China within Chinese

---

<sup>32</sup> 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.

<sup>33</sup> Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People’s Republic of China] (issued by the Standing Committee of the National People’s Congress on 11 July 2016, came into force on 1 June 2017).

<sup>34</sup> 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).

<sup>35</sup> 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);

<sup>36</sup> 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).

<sup>37</sup> D. Hanlin, ‘The System Position and Protection of Personal Information Right in General Provisions of the Civil Law’, *US-China Law Review* 2018/3, p. 153–154; B. Qu, C. Huo, ‘Privacy, National Security, and Internet Economy: An Explanation of China’s Personal Information Protection Legislation’, *Frontiers of Law in China* 2020/3, p. 364; E. Pernot-Leplay, ‘China’s Approach on Data Privacy Law: A Third Way between the U.S. and the EU?’, *Penn State Journal of Law and International Affairs* 2020/8, p. 53–54; Y. Shao, ‘Personal Information Protection: China’s Path Choice’, *US-China Law Review* 2021/18, p. 236–238.

territory.<sup>38</sup> Therefore, all data controllers<sup>39</sup> running their business activity (partially) in China – like companies within the ByteDance Group – fall under the duty to store data created in China locally.<sup>40</sup> Because of this, practically any transfer of personal data from Chinese territory abroad (to the EU/EEA) requires prior authorization under the Cyberspace Administration of China Data Transfer Guidelines.<sup>41</sup>

44. 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.<sup>42</sup> As a result,

---

<sup>38</sup> **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]

<sup>39</sup> That is the conclusion that may be drawn from **Article 31 CSL:** *“The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the critical information infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the critical information infrastructure that will result in serious damage to state security, the national economy and the people’s livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council. The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.”* (emphasis added)

[国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系]

<sup>40</sup> 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.

<sup>41</sup> Shuju Chujiing 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/>

<sup>42</sup> G. Greenleaf, ‘China Issues a Comprehensive Draft Data Privacy Law’, *Privacy Laws & Business International Report* 2020/168, p. 12; G. Greenleaf, ‘China’s Completed Personal Information Protection Law: Rights Plus Cyber-security’, *Privacy Law & Business International Report* 2021/20-23 p. 4.



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

45. Second, there is a very high risk that Chinese authorities will request and obtain (unlimited) access to personal data processed by Chinese companies.<sup>43</sup> 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.<sup>44</sup> 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.<sup>45</sup>
46. Chinese laws, such as the National Security Law (hereinafter: "NSL"),<sup>46</sup> and the National Intelligence Law (hereinafter: "NIL")<sup>47</sup> but also the DSL,<sup>48</sup> are treated as a general legal basis for Chinese authorities' to obtain access to any personal data.<sup>49</sup> 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:

---

<sup>43</sup> Cf. concerns raised by Belgian authorities over alleged espionage activity of Alibaba in Europe ([Link](#)).

<sup>44</sup> 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.

<sup>45</sup> 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.

<sup>46</sup> 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).

<sup>47</sup> 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).

<sup>48</sup> Article 35 DSL.

<sup>49</sup> 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](https://www.hrw.org/sites/default/files/media_2023/03/Letter%20to%20House%20Committee%20on%20TikTok%20-%20web.pdf); T. Giladi Shtub, M.S. Gal, 'The Competitive Effects of China's Legal Data Regime', *Journal of Competition Law and Economics* 2022/4, p. 11.

(a) Article 35 DSL: *“As needed for maintaining national security or investigating crimes, a public security authority or national security authority shall legally pull data in accordance with relevant provisions issued by the state and by strictly following approval procedures, and the relevant organizations and individuals shall provide cooperation.”*<sup>50</sup> 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.<sup>51</sup> (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”.*<sup>52</sup> (emphasis added)

47. As a result, the processing by Chinese national law enforcement and/or national security authorities is not based on clear, precise and accessible rules, necessity and proportionality with regard to legitimate interests pursued are not demonstrated, the processing is not subject to independent supervision and there are no effective remedies available to the Complainant (or other EU data subjects).<sup>53</sup>

48. 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.

---

<sup>50</sup> [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].

<sup>51</sup> See by analogy with the US Cloud Act: <https://www.justice.gov/criminal/cloud-act-resources>

<sup>52</sup> 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。

<sup>53</sup> WP29 Adequacy Referential, WP254/01 (endorsed by the EDPB: [link](#), under 15), p. 9.



49. Although the Respondent has 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

50. It is almost impossible for a foreign data subject to exercise his/her rights under the PIPL<sup>54</sup> or the Chinese Civil Code.<sup>55</sup>

51. First, there is no dedicated, independent and competent data protection authority in China.<sup>56</sup> The CAC plays an important role in Chinese data protection law,<sup>57</sup> although for some provisions it is very difficult to indicate which authority is actually responsible for a particular task.<sup>58</sup> It is worth emphasising that the CAC is closely related to the State Council,<sup>59</sup> 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 139<sup>th</sup> position (out of 142 countries) within the category of fundamental rights protection<sup>60</sup> and the 132<sup>nd</sup> position in category of restraints imposed by the courts on government powers.<sup>61</sup> When it comes to data protection, Chinese courts are not free from political pressure. As a result, the current political needs may prevail

---

<sup>54</sup> 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).

<sup>55</sup> Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code 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.

<sup>56</sup> G. Greenleaf, S. Livingston, 'China's New Cybersecurity – Also a Data Privacy Law?', *Privacy law & Business International Report* 2016/144, p. 8

<sup>57</sup> 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.

<sup>58</sup> R. Creemers, 'China's Emerging Data Protection Framework', *Journal of Cybersecurity* 2022/8, p. 14.

<sup>59</sup> 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.

<sup>60</sup> The World Justice Project Rule of Law Index ([link](#)).

<sup>61</sup> The World Justice Project Rule of Law Index ([link](#)).

over the rights and freedoms of the data subjects.<sup>62</sup> 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.<sup>63</sup>

53. Third, when Chinese law enforcement or national security authorities request access to personal data, these Chinese authorities follow the “black box” route,<sup>64</sup> making it impossible for a data subject, to understand how exactly such requests have been or will be granted.<sup>65</sup> 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 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.<sup>66</sup> 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.<sup>67</sup>

---

<sup>62</sup> 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

<sup>63</sup> 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

<sup>64</sup> W. Chaskes, ‘The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet’, *Washington & Lee Law Review* 2022/1169, p. 1182.

<sup>65</sup> 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>.

<sup>66</sup> P. Cai, L. Chen, ‘Demystifying Data Law in China: A Unified Regime of Tomorrow’, *International Data Privacy Law* 2022/5, p. 79.

<sup>67</sup> 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.

### **4.1.3 Conclusion: TikTok 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.<sup>68</sup>
56. Article 44 GDPR requires the Respondent 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.<sup>69</sup> 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.<sup>70</sup>

## **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 HDPAs take (among others) the following urgent actions:
- *First*, fully investigate the matter under Article 58(1) GDPR.
  - *Second*, **immediately order the suspension of data flows to China** under Article 58(2)(j) GDPR regarding the transfer of the Complainant's and other European users' data to China as it does not provide essentially equivalent level of data protection under Article 44 and 46 GDPR.
  - *Third*, order the Respondent's to 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.

### **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:

---

<sup>68</sup> Cf. EDPB Recommendations 01/2020, para 72.

<sup>69</sup> CJEU C-311/18 (*Schrems II*), para. 101-104.

<sup>70</sup> EDPB Recommendations 01/2020, para 75.

*“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.

### **Investigation under Article 58(1) GDPR**

62. Given that some of the details of the processing of the Complainant’s personal data by the Respondent are unclear, we hereby request a full investigation of the HDPA 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 TikTok Technology Limited and ByteDance Group, (and therefore the roles of the parties), in particular with regard to the processing of the Complainant’s personal data by TikTok 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.

### **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 TikTok 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.

### **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 imposes 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 C093-04** or [REDACTED].