Dr Theo Bertram,
VP Government Relations and Public Policy - Europe,
TikTok,
One London Wall 6th Floor
London EC2Y 5EB

Darren Jones MP,
House of Commons,
London.
SW1A 0AA

14th July 2022

Dear Darren,

As discussed, I am writing to you in your role as Chair of the BEIS Select Committee to set out in a single letter a comprehensive response to the recent report by BuzzFeed about access to U.S. citizens' TikTok user personal data by employees based in China.

**Approach to data governance in the U.S.**

Before explaining our approach to data governance in the U.K., I want to provide a bit more context on the BuzzFeed article. The article relates to discussions about our efforts to strengthen data security in the U.S. and so, by way of background, I hope it is helpful to quote directly from a letter our CEO, Shou Zi Chew, has sent to U.S. Senators on 30th June on this topic:

*"For well over a year, we've been pursuing a multi-pronged initiative called "Project Texas" to strengthen the company's data security program. Security experts can confirm that these initiatives are often painstaking and complex, even with expert assistance from world-class companies like Oracle and Booz Allen. Some people working on these projects do not have visibility into the full picture, working on a task without realizing that it's a single step in a much bigger project or a test to validate an assumption.*

*That's critical context for the recordings leaked to BuzzFeed, and one thing their reporting got right: the meetings "were in service of Project Texas's aim to halt this data access."*
*The broad goal for Project Texas is to help build trust with users and key stakeholders by improving our systems and controls, but it is also to make substantive progress toward compliance with a final agreement with the U.S. Government that will fully safeguard user data and U.S. national security interests. We have not spoken publicly about these plans out of respect for the confidentiality of the engagement with the U.S. Government, but circumstances now require that we share some of that information publicly to clear up the errors and misconceptions in the article and some ongoing concerns related to other aspects of our business.*

*While we are disappointed that leaks have put us in this position, we are pleased to share the substantial progress on our objectives. As we recently reported, we now store 100% of U.S.*

*user data by default in the Oracle cloud environment, and we are working with Oracle on new, advanced data security controls that we hope to finalize in the near future. That work puts us closer to the day when we will be able to pivot toward a novel and industry-leading system for protecting the data of our users in the United States, with robust, independent oversight to ensure compliance."*

You can find further information about the approach to data governance we have taken in the U.S., including the announcement that we now store 100% of U.S. user data by default in the Oracle cloud environment, here.

**Approach to data governance in the U.K. and EEA**

TikTok's data governance strategy is based on aligning with local requirements and values. U.K. data is not part of our work in the U.S. with Oracle, but our plans in Europe (including the U.K.) are aligned with the same principle of accountability guiding our work with Oracle.

Given the strong regulatory oversight already in place through the GDPR, our approach in the EEA and U.K. is based on our commitment to:

- Store European TikTok user data locally, with our new data centre operations in Ireland due to be operational in 2023;
- Minimise data flows outside of the region; and
- Strictly limit the number of employees with any access to data to those who need it to do their job.

**European Data Centre Operations**

In your letter of 12th July, you mentioned you recalled there were plans to store U.K. and E.U. citizen’s date on U.K. or E.U. located servers. This is correct.

EEA and U.K. user data is currently stored in the U.S. and Singapore. As part of our approach to data governance, we announced in April 2022 that we had signed a contract for a data centre in Dublin to enable us to store U.K. & EEA user data locally.

Working with an established third-party service provider on a site that is under construction, our data centre operations will commence in early 2023, ramping up throughout the rest of that year.

You also asked about the types of data being stored in these locations. Our latest Privacy Policy (soon to be effective), lists the types of data which we collect and store and contains a section entitled "Our Global Operations and Data Transfer'.

**Access to data from outside the U.K. and EEA**

In your letter you asked us whether employees based in China can access U.K. citizens' data. As set out in our approach to data governance above, our strategy is based on minimising data flows outside of the U.K. and EEA region and strictly limiting the number of employees with access to data to those who need it to do their job. However, some limited and controlled employee data access remains necessary to support this global community, ensure interoperability of the platform to connect our global community, and make their experience of TikTok enjoyable and safe.

The important point is we ensure that U.K. and EEA users' data is afforded an equivalent level of data protection to that in the EEA and the U.K. for data transfers outside the region. Where data transfers outside of the region are required, we rely on approved methods for data being transferred from the U.K. and EEA, such as standard contractual clauses. We also employ a range of complementary technical, contractual and organisational measures.

This is something we've been open about - for example, you will recall that I told the Joint Committee on the Draft Online Safety Bill last year that:

*"To make the product function and to make the product safe, we have people all around the world. There will be some engineers in China as well, potentially. The rules on who can access data from anywhere in the world across regions are strictly controlled. You can access data only if you have the right permissions to access that data, and only for a limited time and only for the correct data that you need to access. All of that is strictly supervised and audited. We know that there are concerns for all of these processes in general. We are probably the app that has been the most scrutinised in 2020. These issues have all been very thoroughly investigated by external experts and national security teams, and when they have had a look at how we work and operate and what those processes are, they have come to the conclusion that there is no national security risk at all."*

In relation to the element of your question about other ByteDance subsidiaries, I hope it is helpful to again quote from our CEO's response to US Senators of 30th June:

*"Do any Douyin employees have any access to American user data or a role in shaping TikTok's algorithm?*

*ByteDance developed the algorithms for both Douyin and TikTok, and therefore some of the same underlying basic technology building blocks are utilized by both products, but TikTok's business logic, algorithm, integration, and deployment of systems is specific to the TikTok application and separate from Douyin."*

Finally, for the avoidance of doubt, it is important to note that we have never been asked to provide TikTok user data to the Chinese Government, nor would we if asked. More information about government requests for user data we receive across the world is available in our Information Request Reports here.

I hope the above is helpful to you and the Committee. We look forward to continuing to have an open and constructive relationship with the Committee on all aspects of our platform as we continue provide a safe, welcoming, and enjoyable experience for our community.

Yours sincerely,

**Dr Theo Bertram**
**VP Government Relations and Public Policy - Europe**