

## From Microsoft Belgium:

We understand that you have some questions and concerns relating to the impact of the Cloud Act on our enterprise services. You'll find hereafter some explanations relating to the Cloud Act but also, more generally, relating to our duties to co-operate with justice and police co-operation worldwide, as we think that it is important to give the full picture in order to allow you to better understand the precise impact of the Cloud Act.

- Microsoft is obviously bound to respect the legal obligations that apply to its activities, whether it be obligations that follow from U.S. law, Belgian law, EU law, etc. Consequently, Microsoft is also bound to respond to legally valid requests from judicial authorities, e.g. in the context of criminal investigations, whether it be U.S. or other authorities (to the extent that our activities fall under the scope of these legal regimes). As Microsoft, we consider it important to create transparency regarding the scope of our co-operation in this area of judicial requests, which is also why we have chosen to publish non-confidential information on our trust pages <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr>. Hereafter, we summarize the most important principles that apply to these judicial requests.
- First of all, when police or justice authorities contact Microsoft to request access to data of Microsoft's enterprise customers, Microsoft will always refer the authority to the customer. This is also logical as it is the enterprise customer who owns or controls the data. This approach is also described in our Online Service Terms, see <http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31> ("*Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer.*"). The U.S. authorities also endorse this approach and follow this way of working, see e.g. the instructions that the DOJ issued in December 2017 to U.S. prosecutors <https://www.justice.gov/criminal-ccips/file/1017511/download>.
- It is also very important to note that the absolute majority of judiciary requests that Microsoft receives, be it from U.S. authorities or other, relate to our consumer products (e.g. outlook, msn, skype, ...), not to the cloud products offered to enterprise customers (like Azure or Office 365). By way of illustration, and as can be read on our trust pages, out of the 9385 judiciary requests that Microsoft received in 2017 from U.S. authorities, there were only 24 cases where Microsoft ultimately handed over data from enterprise cloud customers (see <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr>, FAQ under the question "*How many enterprise cloud customers are impacted by law enforcement requests?*"). More importantly even, in any event for Belgian customers, is that out of these 9385 requests for 2017, **there was not a single**

**extraterritorial request, meaning that there was no request covering an enterprise customer (> 50 seats) outside the U.S..**

- By the way, the number of judiciary access requests that is coming from U.S. authorities is proportionally rather low as compared to other, smaller countries : for the 2nd half of 2017, we had less than 4000 requests from US compared to approx. 3600 from UK or 3400 from Germany.
- Based on the above information, we hope that you will understand that it is highly unlikely that Microsoft will ever be confronted with a judicial request from U.S. authorities to give access to customer data belonging to an enterprise customer. Should such event nonetheless occur, and assuming that Microsoft would not be able to convince the authorities to address their request directly to the enterprise customer (e.g. in the equally unlikely case where the customer itself would be object of the criminal investigation by the authorities), Microsoft will first make an assessment as to whether the judiciary request is legally valid under the relevant applicable legal regimes, including the Belgian and the EU law, and where relevant defend the rights of its customers in court.
- In this respect, the traditional framework for judiciary co-operation between different countries (which is based on Mutual Legal Assistance Treaties or MLAT) foresees that a foreign authority cannot send a judiciary request directly to a private person abroad, but needs to go via the authorities of the country of the private party. This principle also applies under the MLAT concluded between U.S. and Belgium in January 1998. And Microsoft defended this approach in the NY warrant case (a case which related to a consumer account). We must now see whether/how this principle will evolve with the arrival of the Cloud Act.

The Cloud Act foresees that the U.S. can conclude a new type of bilateral judiciary agreements with foreign states (see <https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/>) and that US authorities can submit requests to US companies also when data is located outside of the US. Awaiting the conclusion of such new bilateral agreements, in the unlikely event where Microsoft would receive a judiciary request from US authorities for data belong to an enterprise customer abroad, Microsoft would have to comply with this request – obviously subject to a legality assessment. In that respect, within the EU, article 48 of the GDPR provides that any judgment or decision from a third country (i.e. non EU country) requiring a company to transfer personal data may only be recognised or enforceable if based on an international agreement, such as a mutual legal assistance treaty between the requesting third country and the Union or a Member State.

- For completeness' sake, we finally note that if Microsoft is confronted with a request for access to the data of an enterprise customer, it will always notify the customer thereof - unless if legally prohibited. This is again

reflected in our Online Service Terms, see <http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31> (*Upon receipt of any other third-party request for Customer Data, Microsoft will promptly notify Customer unless prohibited by local law. Microsoft will reject the request unless required by local law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.*)