

ADEQUATE LEVELS OF PROTECTION FOR LEASEWEB USA, INC.
IN ITS ROLE AS DATA PROCESSOR UNDER THE GDPR IN THE UNITED STATES

Given the EU Court of Justice's ("CJEU") July 16, 2020, judgment in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* ("Schrems II"), Leaseweb USA, Inc. ("Leaseweb USA") provides this document to assist you in determining that there is an adequate level of protection for personal data transferred to Leaseweb USA in the United States.¹

I. OVERVIEW

The information in this document relates ONLY to Leaseweb USA—Although Leaseweb USA's parent entity, Leaseweb Global B.V., and Leaseweb's global headquarters are located in Amsterdam, The Netherlands, Leaseweb USA operates independently and does not access or otherwise process data on behalf of any other Leaseweb Sales Entity. If you have entered into an Sales Contract with or are otherwise obtaining services from any other independent Leaseweb Company, the forms of U.S. legal process addressed in the Schrems II judgment do not apply to such other independent Leaseweb Sales Entity or Headquarters in Amsterdam processing of your data, that is because obviously such non-U.S. Leaseweb Headquarters and other non US-Leaseweb Sales Entities operate and process data outside of the United States and would not be eligible to receive U.S. surveillance orders.

- a) **Leaseweb USA's under its technical and organizational safeguards mitigate the CJEU's surveillance concerns**—As discussed in further detail in Part II of this document, the primary concerns expressed by the CJEU in the *Schrems II* judgment about upstream surveillance under Section 702 of the Foreign Intelligence Surveillance Act ("FISA § 702") and U.S. Executive Order 12333 ("EO 12333"), either do not apply at all to Leaseweb USA's processing of personal data within the United States, or if to a certain extent applicable will be may be mitigated by technical and organizational safeguards customers can employ or that are used by Leaseweb USA.
- b) **Leaseweb USA is committed to providing adequate levels of protection for personal data in accordance with the GDPR**—Leaseweb USA will continue to monitor the implications of the CJEU's invalidation of the EU-US Privacy Shield (and the applicable regulatory guidance) and will implement such additional technical and organizational safeguards as may be required to enable the free flow of global data and the adequate protection of personal data.

II. LEASEWEB USA'S TECHNICAL AND ORGANIZATIONAL SAFEGUARDS TO ADDRESS U.S. SURVEILLANCE CONCERNS

a. *Leaseweb USA is not eligible to receive "upstream" or bulk surveillance orders under FISA § 702*

Like all other IaaS cloud hosting providers in the United States, Leaseweb USA is a remote computing service ("RCS") (as defined in Section 2711 of Title 18 U.S.C.) when it provides services to customers. It is thus possible the United States government could serve a targeted directive on Leaseweb USA under FISA § 702.

However, Leaseweb USA is not eligible to receive the type of order that was of principal concern to the CJEU in the *Schrems II* decision—meaning, a FISA § 702 order for "upstream" surveillance.

The way that the U.S. Government has interpreted and applied FISA § 702, it uses upstream orders only to target market providers that have traffic flowing through their internet

¹ Leaseweb USA provides the information contained herein to the best of its knowledge as of January 2021.

backbone and that carry traffic for third parties (i.e., telecommunications carriers).² Leaseweb USA does **not** provide such backbone services, as it only carries traffic involving its own customers as a side product of the IaaS hosting. As a result, Leaseweb USA is not eligible to receive the type of order principally addressed in, and deemed problematic by, the *Schrems II* decision.

b. Leaseweb USA does not and cannot be ordered to assist U.S. authorities in their bulk collection of information under Executive Order 12333

Leaseweb USA does not provide any assistance to U.S. authorities conducting surveillance under EO 12333.

EO 12333 does not provide the U.S. government the ability to order or demand companies to provide assistance for the bulk collection of information and Leaseweb USA will not do so voluntarily. As a result, Leaseweb USA does not, and cannot be ordered to, take any action to facilitate the type of bulk surveillance under EO 12333 that was referred to in the *Schrems II* decision and deemed problematic by the CJEU. If the U.S. government were to ask Leaseweb USA, either on a voluntary or a compulsory basis, to take any such action to facilitate the government's bulk surveillance activities under EO 12333, Leaseweb USA would decline to do so or otherwise challenge such a request.

c. Leaseweb USA provides Technical and Organizational Safeguards to establish adequate levels of protection

Leaseweb USA provides a range of technical and organizational measures that further defeat the core deficiencies cited in the *Schrems II* decision referred to above in Sections (a) and (b) of this Part II (bulk surveillance under FISA § 702 and bulk interceptions under EO 12333).

Leaseweb USA can work with customers to encrypt: (i) transfers of United Kingdom or European Economic Area data ("UK/EEA Data") between us (i.e., between customer and Leaseweb USA) and by Leaseweb USA internally or to third parties, and (ii) UK/EEA Data when it is in storage or otherwise not in transit. These encryption efforts, if applied, can prevent the acquisition of UK/EEA Data in an intelligible form by governmental authorities and other third parties who may gain physical access to the hosting and computing environment or transmission mechanisms (e.g., servers, wires and cables) while the data is in transmission or in storage. Leaseweb USA can also use secure data transport through TLS 1.2 over HTTPS. This feature can be enabled so that U.S. law enforcement or intelligence authorities will be unable to tamper with or tap into the data transfers between the two end-points (Leaseweb USA and our customers).

Our Customers can take additional steps to ensure your UK/EEA Data is delivered to us in a secure form. We encourage you to do so and can work with you to discuss encryption practices that will be compatible with Leaseweb USA's services.

Leaseweb USA also maintains strict administrative, technical, and physical procedures to protect information stored on its servers. Access to personal information is limited through login credentials to those employees who require it to perform their job functions. In addition, Leaseweb USA uses access controls such as multi-factor authentication, Single Sign

² For more information: See Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014) pp. 35-40, available at <https://fas.org/irp/offdocs/pclomb-702.pdf>.

On, access on an as-needed basis, strong password controls, and restricted access to administrative accounts.

Additionally, as an RCS, Leaseweb USA is subject the Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et seq.* (“**ECPA**”), which provides protection to its customers. For example, ECPA prohibits governmental entities from seeking information about customers of services like Leaseweb USA unless such governmental entities first obtain appropriate legal process, including a court order or search warrant for information other than basic subscriber information. Likewise, both FISA and ECPA provide Leaseweb USA’s customers with redress against the United States government if it improperly obtains information about them. See 18 U.S.C. § 2712.

Further, Leaseweb USA has established and continuous relationships with reputable outside legal counsel experienced in responding to U.S. governmental requests for user data, including U.S. national security requests. It is Leaseweb USA’s policy to escalate any such requests to Leaseweb USA’s own internal Compliance Team and such outside counsel for review. Leaseweb USA intends to use available legal mechanisms to challenge demands for data access using FISA § 702 and any non-disclosure provisions or orders attached thereto.

If you have any questions about the information above, please contact us-privacy@us.leaseweb.com.