CUSTOMER
DATA PROCESSING ADDENDUM

Version: 16 June 2025

1. Parties, Order of Precedence, and Scope

This Data Processing Addendum ("**DPA**") forms part of and is incorporated into: (i) the Wrike Terms of Service, available online at https://www.wrike.com/terms; (ii) the Wrike Terms & Conditions, available online at https://www.wrike.com/legal/enterprise-wmsa; or (iii) the separate written agreement governing use of Wrike's and/or its Affiliates' hosted, on-demand, cloud-based service offerings (the "**Service**") and any related Support Services and Professional Services (collectively, the "**Service Offerings**") (the "**Agreement**") entered by and between you, the Customer (as defined in the Agreement) ("**Customer**", "**you**", or "**your**") and Wrike, Inc. or the Affiliate identified in the signature block below from whom you have purchased the Service ("**Wrike**", "**we**", "**us**", or "**our**"). You and Wrike may be individually referred to as a "**Party**" and us, collectively, as the "**Parties**."

This DPA reflects the Parties agreement with regard to the Processing of Personal Data by Wrike solely on your behalf when performing the Service Offerings. Capitalized terms used but not defined herein have the meaning as the same or substantially equivalent term in the Agreement. In the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA shall control. In the event of a conflict between the terms of this DPA and the 2021 EU Standard Contractual Clauses, the UK SCC Addendum, and/or Swiss SCCs (if applicable), the terms of the 2021 EU Standard Contractual Clauses, the UK SCC Addendum and/or the Swiss SCCs (as applicable) shall control to the extent applicable.

Wrike is the Controller of Personal Data relating to its Customers, end users, and website visitors. This is further explained in our Privacy Policy located at https://www.wrike.com/privacy. Wrike is the Processor of Personal Data submitted by or on behalf of Customer to Wrike in connection with our performing the Service Offerings, and Wrike Processes this Personal Data solely on its Customers' behalf in accordance with this DPA.

2. Definitions

"**Affiliate**" means any parent, subsidiary, or other affiliate of Wrike, Inc. that may Process or assist in the Processing of your Personal Data under this DPA.

"**Applicable Data Protection Laws**" means, with respect to a Party, all applicable data protection and

privacy legislation which applies to such Party relating to its Processing of Personal Data, including without limitation (i) the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"), (ii) in respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Act on Data Protection and its Ordinance ("**Swiss FADP**"); (iv) the California Consumer Privacy Act (as amended and together with its regulations, the "**CCPA**"), (v) other U.S. state privacy laws, including for example, solely to the extent applicable, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Oregon Consumer Privacy Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act; (vi) any laws or regulations implementing or supplementing the foregoing; and (vii) any other international, federal, state, provincial and local privacy or data protection laws, rules, regulations, legally binding directives and governmental requirements currently in effect and as they become effective that apply to the Processing of Personal Data under this DPA.

"**Customer Account**" means an account required for Customer to access and use the Service. Following expiration, termination or suspension of Service, Wrike may convert such Customer Account to a free Customer Account (if available for the particular terminated, expired, or suspended Service Subscriptions), such Customer Account thereafter referred to herein as a "**Free Customer Account**."

"**Customer Content**" means any content, including Customer Data, uploaded to your Customer Account for storage or other Processing by Wrike in performing the Service Offerings or any content in your computing environment to which Wrike is provided access in order to perform the Service Offerings.

"**Customer Data**" means all data or information submitted by or on behalf of Customer to the Service, but does not include Aggregated Anonymous Data. "**Aggregated Anonymous Data"** means the metadata and usage data of Customer and/or its end users collected or otherwise made available through the Service so that the results are non-personally identifiable with respect to Customer or end users.

"**Effective Date**" of this DPA shall be the later date between the effective date of the Agreement and the date of Wrike's signature below.

"**2021 EU SCCs**" or "**2021 EU Standard Contractual Clauses**" means the contractual clauses annexed to the EU Commission Decision 2021/914/EU or any successor clauses approved by the EU Commission.

"**Personal Data**" means any Customer Content Processed in connection with our performance of Service Offerings that can identify a unique individual, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of individuals or as such information may be otherwise defined under

Applicable Data Protection Laws.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed in order to perform the Service Offerings that compromises the security of the Personal Data.

"**Service**" means Wrike's and/or its Affiliates' hosted, on-demand, cloud-based service offerings.

"**Sub-Processor**" means any third party Wrike engages to assist with the Processing of Personal Data for the performance of the Service Offerings under the Agreement.

"**Swiss SCCs**", means the 2021 EU SCCs, modified for transfers subject to Swiss data protection law pursuant to guidance from the Swiss Federal Protection and Information Commissioner as set forth below in the DPA.

"**UK SCC Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (vB1.0 or any subsequent version) issued by the UK Information Commissioner's Office.

Capitalized terms used but not defined in this DPA (e.g. "Controller," "Data Subject," "Process/Processing," Processor") shall have the same meaning as set forth in the Agreement or Applicable Data Protection Laws, provided that unless otherwise stated, "Controller" shall be deemed to include "Business," "Data Subject" shall be deemed to include "Consumer," and "Processor" shall be deemed to include "Service Provider."

3. Roles as Data Controller and Data Processor

This DPA will apply when you are (or are acting on behalf of) the Controller of the Personal Data, and not when Wrike is acting as a Controller. You are responsible for complying with your obligations under Applicable Data Protection Laws with respect to your provision of Personal Data to Wrike and your use of the Service, including without limitation obtaining any consents, providing any notices, or otherwise establishing the required legal basis of Processing, and responding swiftly to any enquiries from any relevant data protection authorities in accordance with Applicable Data Protection Laws. You will limit Wrike's access to Personal Data to the minimum necessary for it to perform the Service Offerings and will not provide Wrike with access to any Personal Data not necessary to perform the Service Offerings that would subject Wrike to Applicable Data Protection Laws.

Wrike is a Processor with respect to such Personal Data, and when you act as a Processor of Personal Data, in which case Wrike is your Sub-Processor. Wrike is responsible for complying with its obligations under Applicable Data Protection Laws that apply to its Processing of Personal Data under the Agreement and this DPA.

For the avoidance of doubt, each Party is responsible for complying with the obligations applicable to it under Applicable Data Protection Laws, and Wrike is not responsible for your compliance with the obligations applicable to you under such laws.

4. Wrike's Purpose of Processing

Wrike will Process Personal Data only for the purposes of performing the Service Offerings in accordance with your lawful written instructions (which consist of this DPA, the rest of the Agreement, and your use of settings that Wrike makes available in the Service). Wrike will not disclose Personal Data in response to a subpoena, judicial or administrative order, or other binding instrument (a "**Demand**") unless required by law. Wrike will promptly notify you of any Demand unless prohibited by law and provide you reasonable assistance to facilitate your timely response to the Demand.

5. Data Subjects and Categories of Personal Data

You determine the Personal Data to which you provide Wrike access to in order to perform the Service Offerings. Because you control the content, this may involve the Processing of Personal Data of any category of your Data Subjects, such as:

- Customers and end users
- Employees and applicants
- Suppliers, agents, and contractors
- Others

Because you control the content you provide to Wrike in connection with our performing the Service Offerings, the Processing of your Personal Data may include any category of Personal Data, such as:

- Contact information such as name, address, telephone number, email address, and fax number.
- Customer service records
- Employment information such as employer, job title and function
- Goods or services purchased
- Other Personal Data

6. Sub-Processing

Authorisation of Sub-Processors and Affiliates: Subject to the terms of this DPA, you generally authorize Wrike to engage Sub-Processors and Affiliates to Process Personal Data in support of Wrike's performing of the Service Offerings. These Sub-Processors and Affiliates are bound by written agreements that require them to provide at least the level of data protection required of Wrike by the Agreement and this DPA. Wrike is responsible for such Sub-Processors' and Affiliates' acts and omissions with respect to this DPA as if such acts and omissions were Wrike's own.

A list of Sub-Processors and Affiliates, as well as a mechanism to obtain notice of any updates to the

list, are available at https://www.wrike.com/legal/subprocessors-list/. By entering into this DPA, you authorize Wrike to continue to use the Sub-Processors and Affiliates listed therein.

Change Notifications: At least twenty one (21) calendar days (the "**Notice Period**") before authorizing any new Sub-Processor to access Personal Data, Wrike will update the list of Sub-Processors and Affiliates. To receive notice of any new or replacement Sub-Processor or Affiliate on this list, you must click the 'Subscribe to updates' button on https://www.wrike.com/legal/subprocessors-list/ and enter your email address.

Right to Object: If you have an objection to a new Sub-Processor or Affiliate based on reasonable grounds, you may object to the new Sub-Processor or Affiliate by notifying Wrike at privacy@team.wrike.com within seven (7) calendar days after Wrike's above-mentioned notice regarding the change. In such case Wrike will consider any such request but shall in no way be restricted in proceeding with such appointment. Wrike will inform you by five (5) calendar days before expiration of the Notice Period if it has determined it will not accommodate the objection, in which case you may terminate the applicable Service Offerings without penalty by providing to Wrike, before the end of the Notice Period, written notice of termination that includes an explanation of the grounds for non-approval.

- If the affected Service Offerings are part of a suite (or similar single purchase of services), then, at your option, any such termination will apply to the entire suite.
- After such termination, you shall remain obligated to make all payments required under what would have been the remainder of the term of any purchase order or other contractual obligation with Wrike and/or a Wrike reseller and shall not be entitled to any refund or return of payment from Wrike and/or the Wrike reseller.

7. International Transfer of Personal Data

Wrike Processes Personal Data on a global basis and may transfer Personal Data to the United States and/or to other countries to perform the Service Offerings, provided that Wrike makes such transfers in accordance with Applicable Data Protection Laws. Wrike will follow the requirements of this DPA regardless of where Wrike stores or otherwise Processes Personal Data.

Wrike has certified that it adheres to the EU-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US DPF, and the Swiss-US Data Privacy Framework program (Swiss-US DPF) (collectively, the "**Data Privacy Framework**") as set forth by the US Department of Commerce. To the extent Wrike in the United States receives Personal Data that is subject to the data protection laws of the European Economic Area, United Kingdom, or Switzerland, it receives such Personal Data pursuant to, and will handle such Personal Data in compliance with, the Data Privacy Framework and will inform you if it can no longer provide this level of protection.

Regardless, to the extent legally required, the 2021 EU Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict, and they will be deemed completed as follows:

a. Wrike, the importer, acts as your Processor with respect to the Personal Data subject to the 2021 EU Standard Contractual Clauses. To the extent you are a controller of such Personal Data, Module 2 applies, and to the extent you are a Processor of it, Module 3 applies. The Parties' contact information is set forth in Appendix A to this DPA.

b. Clause 7 (the optional docking clause) is included.

c. Under Clause 9 (Use of Sub-Processors), the Parties select Option 2 (General written authorization). The initial list of Sub-Processors is set forth at https://www.wrike.com/legal/subprocessors-list, and Wrike shall update that list at least twenty-on (21) calendar days in advance of any intended additions or replacements of Sub-Processors.

d. Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

e. Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law of France.

f. Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of France.

g. Annexes I and II of the 2021 EU Standard Contractual Clauses are set forth in Appendix A to this DPA.

h. Annex III of the 2021 EU Standard Contractual Clauses (List of Sub-Processors where prior written consent is required) is inapplicable.

With respect to Personal Data for which the UK GDPR governs the transfer, to the extent legally required, the UK SCC Addendum forms part of this DPA and takes precedence over the rest of this DPA to the extent of any conflict and shall be deemed completed as follows (with capitalized terms not defined elsewhere having the definition set forth in the UK SCC Addendum):

a. Table 1 of the UK SCC Addendum: The Parties, their details, and their contacts are those set forth in Appendix A to this DPA.

b. Table 2 of the UK SCC Addendum: the "Approved EU Standard Contractual Clauses" shall be the 2021 EU Standard Contractual Clauses as set forth above this DPA.

c. Table 3 of the UK SCC Addendum: Annexes I(A), I(B), and II are in Appendix A to this DPA, and Annex III is inapplicable.

d. Table 4 of the UK SCC Addendum: neither Party may exercise the right set forth in Section 19 of the UK SCC Addendum.

With respect to Personal Data for which the Swiss FADP governs the transfer, the Standard Contractual Clauses shall be deemed to have the following differences to the extent required by the Swiss FADP:

a. References to the GDPR in the 2021 EU Standard Contractual Clauses are to be understood as references to the Swiss FADP insofar as the data transfers are subject exclusively to the Swiss FADP and not to the GDPR.

b. The term "member state" in 2021 EU Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses.

c. Under Annex I(C) of the 2021 EU Standard Contractual Clauses (Competent supervisory authority):

    i. Where the transfer is subject exclusively to the Swiss FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

    ii. Where the transfer is subject to both the Swiss FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the Swiss FADP, and the supervisory authority is as set forth in the 2021 EU Standard Contractual Clauses insofar as the transfer is governed by the GDPR.

8. Requests from Data Subjects

Wrike will make available to you the Personal Data of your Data Subjects and the ability to fulfil requests by Data Subjects to exercise one or more of their rights under Applicable Data Protection Laws in a manner consistent with Wrike's role as a Data Processor. Wrike will provide reasonable assistance to assist with your response. If Wrike receives a request directly from your Data Subject to exercise one or more of their rights under Applicable Data Protection Laws, Wrike will direct the Data Subject to you unless prohibited by law.

9. Security

Wrike shall implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Data against misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such security practices are set forth in the Wrike Information Security Addendum which is available at https://learn.wrike.com/enterprise-winfosec/. Wrike reserves the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of the Service Offerings.

Wrike employees are bound by appropriate confidentiality agreements and required to take regular data protection training as well as comply with Wrike corporate privacy and security policies and procedures.

10. Personal Data Breach

Wrike shall notify you without undue delay and in accordance with Applicable Data Protection Laws, but in no event not to exceed seventy-two (72) hours, after becoming aware of a Personal Data Breach involving Personal Data in Wrike's possession, custody or control. Taking into account the nature of Processing and information available to Wrike at the time of any such breach, such notification shall at least: (i) describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of your Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) describe the likely consequences of the Personal Data Breach; and (iii) describe the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects. you will coordinate with Wrike on the content of any public statements or required notices to individuals and/or Supervisory Authorities.

11. Your Instructions and Providing Information & Assistance

Wrike will promptly inform you if it believes that your instructions are not consistent with Applicable Data Protection Laws, provided that Wrike shall not be obligated to independently inspect or verify your Processing of Personal Data.

Wrike will provide you with information reasonably necessary to demonstrate Wrike's compliance with this DPA and assist you in enabling your compliance with your obligations under Applicable Data Protection Laws, including without limitation obligations to implement appropriate data security measures, carry out a data protection impact assessment and consult the competent Supervisory Authority (taking into account the nature of Processing and the information available to Wrike), and as further specified in this DPA.

12. Return and Deletion of Personal Data

Following expiration or termination of the Agreement, Wrike may immediately deactivate your Customer Account or may convert your Customer Account to a Free Customer Account. You may not be able, or may have limited ability, to export Customer Data, including your Personal Data, after deactivation of your Customer Account or conversion to a Free Customer Account and it is your sole liability to export your Customer Data from your Customer Account prior to expiration or termination of the Agreement. If you request your Customer Data within thirty (30) days of expiration or termination of the Agreement, Wrike will make available to you an electronic copy of your Customer Data for an additional fee at Wrike's then-current rates. After such 30-day period, Wrike shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited or your Customer Account is converted to a Free Customer Account, delete all Customer Data in its production Service environment in accordance with Wrike's then-current

practices. Wrike will automatically delete a converted Free Customer Account and any remaining Customer Data after such Free Customer Account has been inactive for one-hundred-eighty (180) days. Notwithstanding, Wrike may retain backup copies of Customer Data for security, backup, or business continuity purposes for a limited period of time in accordance with Wrike's then-current practices. Wrike will continue to comply with the relevant provisions of this DPA until such data has been deleted.

13. Audit

In the event the information you request of Wrike under Section 11 above does not satisfy your obligations under Applicable Data Protection Laws, you may carry out an audit of Wrike's Processing of your Personal Data up to one time per year or as otherwise required by Applicable Data Protection Laws. To request an audit, you must provide Wrike with a proposed detailed audit plan three weeks in advance, and Wrike will work with you in good faith to agree on a final written plan. Any such audit shall be conducted at your own expense, during normal business hours, without disruption to Wrike's business, and in accordance with Wrike's security rules and requirements. Prior to any audit, Wrike undertakes to provide you reasonably requested information and associated evidence to satisfy your audit obligations, and you undertake to review this information prior to undertaking any further independent audit. If any of the requested scope of the audit is covered by an audit report issued to Wrike by a qualified third-party auditor within the prior twelve months, then the parties agree that the scope of your audit will be reduced accordingly.

You may use a third-party auditor with Wrike's agreement, which will not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Wrike. If the third party is your Supervisory Authority that applicable law enables it to audit Wrike directly, Wrike will cooperate with and provide reasonable assistance to the Supervisory Authority in accordance with Applicable Data Protection Laws.

You will provide Wrike with a copy of any final report unless prohibited by Applicable Data Protection Laws, will treat the findings as Confidential Information in accordance with the terms of the Agreement (or confidentiality agreement entered into between you and Wrike), and use it solely for the purpose of assessing Wrike's compliance with the terms of the Agreement, this DPA and Applicable Data Protection Laws.

14. CCPA-Specific Provisions

This Section 14 applies in addition to the rest of the DPA solely to the extent that the CCPA applies to Wrike's Processing of Personal Data to perform the Service Offerings. To the extent that the CCPA applies, Wrike will:

- Process Personal Data solely to perform the Service Offerings described in the relevant order as set forth in section 4 of this DPA;
- Not "sell" or "share" Personal Data, as such terms are defined in the CCPA;

- Not retain, use, or disclose Personal Data outside of the direct business relationship between you and Wrike, or for any purpose (including any commercial purpose) not set forth in this DPA or the Agreement;
- Not attempt to re-identify any de-identified Personal Data provided by you;
- Comply with any applicable restrictions under the CCPA on combining the Personal Data with personal information that Wrike receives from, or on behalf of, another person or persons, or that Wrike collects from any interaction between it and any individual;
- Promptly notify you if Wrike determines that it can no longer meet its obligations under this Section 14 or the CCPA; and
- Comply with all applicable sections of the CCPA, including by providing the level of protection required by the CCPA to Personal Data subject to the CCPA.

To the extent that the CCPA applies, you retain the right to (i) ensure that Wrike Processes Personal Data in a manner consistent with the CCPA, and (ii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

Wrike certifies that it understands and will comply with its obligations in this Section 14.

15. Privacy Contact

You may contact the Wrike Privacy Team and Wrike's Data Protection Officer at privacy@team.wrike.com.

16. Term

This Agreement becomes effective upon your authorized use and Wrike's performance of the Service Offerings.

[Signatures Follow]

IN WITNESS WHEREOF, the Parties by the undersigned duly authorized representatives, intending to be legally bound, have executed this Agreement as of the Effective Date

Wrike, Inc.	
By:	
Name:	Caroline Davoust
Title:	Deputy Data Protection Officer
Date:	16 June 2025
Address:	55 West B Street, Floor 4, PMB 2305 San Diego, CA 92101 USA
Notice Copy:	legal@team.wrike.com
Role with respect to Personal Data: Processor	
Security Point of Contact: security@team.wrike.com	

Klaxoon SAS	
By:	
Name:	Caroline Davoust
Title:	Data Protection Officer
Date:	16 June 2025
Address:	Bâtiment Energie B2, 3 avenue de Belle Fontaine Cesson Sévigné, 35510, FR
Notice Copy:	legal@team.wrike.com
Role with respect to Personal Data: Processor	
Security Point of Contact: security@team.wrike.com	

APPENDIX A

STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Customer:

Name: As set forth in the Agreement signature block.
Address: As set forth in the Agreement signature block.
Contact person's name: As set forth in the Agreement signature block.
Contact person's position: As set forth in the Agreement signature block.
Contact Person's contact details: As set forth in the Agreement signature block.
Activities relevant to the data transferred under these Clauses: Obtaining IT services and solutions as described in the Agreement.
Signature and date: As set forth in the Agreement signature block.
Role: Controller.

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: As set forth in the DPA signature block.
Address: As set forth in the DPA signature block.
Contact person's name: As set forth in the DPA signature block.
Contact person's position: As set forth in the DPA signature block.
Contact person's contact details: privacy@team.wrike.com
Data Protection Officer's contact details: privacy@team.wrike.com
Activities relevant to the data transferred under these Clauses: Providing IT services and solutions as described in the Agreement.
Signature and date: As set forth in the DPA signature block.
Role (Controller/Processor): As set forth in the DPA signature block.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred

Please refer to Section 5 of the DPA.

Categories of Personal Data transferred

Please refer to Section 5 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data is required, though the data exporter is capable of uploading any category of personal data.

Technical and organisational security measures are described in the Wrike Information Security Addendum available at https://learn.wrike.com/enterprise-winfosec/.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfers on a continuous basis as needed to perform the Service Offerings.

Nature of the Processing

Receipt, storage, display, and transmission of data.

Purpose(s) of the data transfer and further Processing

Please refer to Section 4 of the DPA.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

Please refer to Section 12 of the DPA.

For transfers to (Sub-) Processors, also specify subject matter, nature and duration of the processing

Please refer to https://www.wrike.com/legal/subprocessors-list/. Transfers on a continuous basis as needed to perform the Service Offerings.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: Irish Data Protection Commission

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: Irish Data Protection Commission

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Irish Data Protection Commission

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and organisational security measures are described in the Wrike Information Security Addendum available at https://learn.wrike.com/enterprise-winfosec/.