

Wrike Data Protection Addendum

This Data Protection Addendum (“DPA”) is entered into as of the Effective Date (defined below) between Wrike, Inc. (“Wrike”) and the entity identified below (“Customer”). Wrike and Customer may each be referred to as a “Party” and or collectively referred to as the “Parties”. This DPA supplements any Order Form entered between Parties and is subject to either (i) the Wrike Terms of Service at <https://www.wrike.com/security/terms>; or (ii) the alternative agreement (if applicable) signed between Parties for the Services (collectively, the “Agreement”). This DPA supplements the Agreement and replaces any prior contractual obligations between the Parties regarding any privacy, security, confidentiality, or data protection obligations relevant to the Personal Data covered by this DPA. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern. The “Effective Date” of this DPA shall be the later date between (x) the Effective Date of the Agreement; or (y) the date of Wrike’s signature below.

Definitions

1. In this DPA:
 - a. “Applicable Law” means all laws, regulations and other legal requirements applicable to either (i) Wrike in its role as provider of the Services or (ii) Customer. This may include, for example, the General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”). Each party is responsible only for the Applicable Law applicable to it.
 - b. “Notification Email Address” means the main email address associated with Customer’s administrator account in the Services and/or as outlined in the signature field below.
 - c. “Personal Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or exfiltration of, or access to, Personal Data.
 - d. “Personal Data” means (i) any information relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies) and (ii) any other information constituting “personal information” as such term is defined in the California Consumer Privacy Act (“CCPA”) (regardless of whether the CCPA applies).
 - e. “Process” and “Processing” mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
 - f. “Services” means Wrike’s hosted and web-based instance subscribed to and administered by Customer and (if applicable) any related professional services provided by Wrike under the Agreement as identified in an Order Form signed by Parties or a Quote signed by Customer.
 - g. “Standard Contractual Clauses” means the document set forth in Annex A.
 - h. “Subprocessor” means any Wrike affiliate or subcontractor engaged by Wrike for the Processing of Personal Data.
2. Capitalized terms not otherwise defined herein will also have the meaning set forth in the Agreement.

Scope and Relationship of the Parties

3. This DPA applies only to the Personal Data that Wrike receives in the Services from Customer or Customer’s Users (including any Collaborators, External Users, and Regular Users as defined in the Agreement). The DPA survives the Agreement for so long as Wrike continues to Process such Personal Data.
4. For such Personal Data, Customer is (or represents that it is acting with full authority on behalf of) the “Controller”, and Wrike is the “Processor”, as such terms are defined in the GDPR (regardless of whether the GDPR applies). If Customer is acting on behalf of another Controller (or on behalf of intermediaries such as other Processors of the Controller), then, to the extent legally permissible:
 - a. Customer will serve as the sole point of contact for Wrike with regard to any such third parties;
 - b. Wrike need not interact directly with any such third party (other than through regular provision of the Service to the extent required by the Agreement); and
 - c. Where Wrike would otherwise be required to provide information, assistance, cooperation, or anything else to such third party, Wrike may provide it solely to Customer; but
 - d. Wrike is entitled to follow the instructions of such third party with respect to such third party’s Personal Data instead of Customer’s instructions if Wrike reasonably believes this is legally required under the circumstances.
5. Customer’s contact details for its various security and privacy related contacts are outlined in the signature field below. Customer agrees to (i) if applicable, provide requisite updates to such contact information by emailing privacy@team.wrike.com, and (ii) maintain accurate contact information in Customer’s Account in the Services.

Customer’s Instructions to Wrike

6. Wrike will retain, use, disclose, and otherwise Process the Personal Data only as described in the Agreement, unless obligated to do

otherwise by Applicable Law. In such case, Wrike will inform Customer of that legal requirement before the Processing unless legally prohibited from doing so. Without limiting the foregoing:

- a. Wrike will not retain, use, disclose, or otherwise Process the Personal Data in a manner inconsistent with Wrike's role as Customer's "Service Provider", as such term is defined in the CCPA (regardless of whether the CCPA applies);
 - b. Wrike will not "sell" the Personal Data, as such term is defined in the CCPA (regardless of whether the CCPA applies);
 - c. Wrike hereby certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them.
7. The details of the Processing are set forth in Appendix 1 to the Standard Contractual Clauses.
 8. Customer will not instruct Wrike to Process Personal Data in violation of Applicable Law. Wrike has no obligation to monitor the compliance of Customer's use of the Services with Applicable Law, though Wrike will promptly inform Customer if, in Wrike's opinion, an instruction from Customer infringes Applicable Law.
 9. The Agreement, including this DPA, along with Customer's configuration of any settings or options in the Services (as Customer may be able to modify from time to time), constitute Customer's complete and final instructions to Wrike regarding the Processing of Personal Data, including for purposes of the Standard Contractual Clauses.

Subprocessors

10. Wrike may subcontract the collection or other Processing of Personal Data in compliance with Applicable Law to provide the Services. Prior to a Subprocessor's Processing of Personal Data, Wrike will impose contractual obligations on the Subprocessor that are substantially the same as those imposed on Wrike under this DPA. Subprocessor security obligations will be deemed substantially the same if they provide a commercially reasonable level of security even if the Subprocessor does not follow the security certifications that Wrike does. Wrike will conduct an annual review of each Subprocessor's security practices.
11. Subprocessors are listed at <https://learn.wrike.com/subprocessor-list/> (the "**Subprocessor List**"). When any new Subprocessor is engaged, Wrike will provide at least 5 business days' notice before the new Subprocessor Processes any Personal Data by adding it to the Subprocessor list, unless exigent circumstances require earlier Processing of Personal Data, in which case they will be added as soon as practicable. If Customer subscribes to updates using the form available on the Subprocessor List webpage mentioned above, Wrike will email Customer notification of the update when Wrike posts it. This paragraph constitutes Customer's consent to the Subprocessor List, as well as any subprocessing under the Standard Contractual Clauses, if they apply. The subprocessor agreements to be provided under Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses, redacted prior to sharing with Customer, and Customer agrees that such copies will be provided by only upon request.
12. Customer's sole recourse if it objects to a Subprocessor will be to terminate Customer's subscription to the Services. Following such termination, Customer will be entitled to a refund of unused prepaid fees only if (a) Wrike breached its obligation to maintain the requisite contract provisions with the Subprocessor, (b) Wrike breached its obligation to conduct an annual security review of the Subprocessor, or (c) the Agreement otherwise provides for a refund. This is without prejudice to any right Customer may have under the Agreement to termination for breach of contract.
13. Wrike remains liable for its Subprocessors' performance to the same extent Wrike is liable for its own performance, consistent with the limitations of liability set forth herein.

Security

14. Wrike will assist Customer in Customer's compliance with the security obligations of the GDPR and other Applicable Law, as relevant to Wrike's role in Processing the Personal Data, taking into account the nature of Processing and the information available to Wrike, by implementing technical and organizational measures that comply with Annex B, without prejudice to Wrike's right to make future replacements or updates to the measures that do not lower the level of protection of Personal Data.
15. Wrike will ensure that the persons Wrike authorizes to Process the Personal Data are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality. Wrike will train its employees annually (and at additional times if appropriate) regarding confidentiality, data security and data use.

Personal Data Breach Notification

16. Wrike will comply with the Personal Data Breach-related obligations directly applicable to it under the GDPR and other Applicable Law. Taking into account the nature of Processing and the information available to Wrike, Wrike will assist Customer in complying with those applicable to Customer by informing Customer of a confirmed Personal Data Breach within 48 hours of becoming aware. Wrike will notify Customer at the Notification Email Address, or at another email address that Customer provides to Wrike in writing (such as the Security Point of Contact or Secondary Security Point of Contact, set forth in the signature field below) for purposes of Personal Data Breach notifications. Any such notification is not an acknowledgement of fault or responsibility. To the extent available, this notification will include Wrike's then-current assessment of the following, which may be based on incomplete information:

- a. The nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;
 - b. The likely consequences of the Personal Data Breach; and
 - c. Measures taken or proposed to be taken by Wrike to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.
17. Nothing shall be construed to require Wrike to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.

Assistance Responding to Data Subjects

18. Taking into account the nature of the Processing, Wrike will assist Customer with the fulfilment of Customer's obligation to honor requests by individuals to exercise their rights under the GDPR and other Applicable Law (such as rights to access their Personal Data) by providing the Service and the self-service functionality described at <https://help.wrike.com/hc/en-us>, as updated from time to time ("Self-Service Tool") and by forwarding to the Notification Email Address any such requests or Personal Data-related complaints that Wrike receives. Wrike will send this within a commercially reasonable timeframe, which shall will not exceed 5 business days if (i) the request or complaint is received through the contact information specified in the Wrike privacy policy that is linked from the home page of wrike.com and (ii) the request or complaint identifies Customer as the Wrike customer to whom it pertains. Additional support relating to data subject requests and complaints may be available and would require mutual agreement on fees, the scope of Wrike's involvement, and any other terms that the Parties deem appropriate. Although it is Customer's responsibility to respond to and honor data subjects' requests in compliance with law, Wrike does not waive any rights under the Agreement to remove content from the Services.

Assistance with DPIAs and Consultation with Supervisory Authorities

19. Taking into account the nature of the Processing and the information available to Wrike, Wrike will provide reasonable assistance to and cooperation with Customer for Customer's performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Wrike, and with related consultation with supervisory authorities, by providing Customer with any publicly available documentation for the relevant Services or by complying with the Audit section below. Additional support for data protection impact assessments or relations with regulators may be available and would require mutual agreement on fees, the scope of Wrike's involvement, and any other terms that the Parties deem appropriate.

Data Transfers

20. Wrike will comply with all Applicable Laws applicable to Wrike in its role as provider of the Services. Customer will comply with all Applicable Laws relevant to use of the Services, including by obtaining any consents and providing any notices required under Applicable Laws for Wrike to provide the Services. Customer will ensure that Customer and Customer's authorized users are entitled to transfer the Personal Data to Wrike so that Wrike and its Subprocessors may lawfully Process the Personal Data in accordance with this DPA.
21. Customer authorizes Wrike and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.
22. As of the Effective Date of this DPA, Wrike is a member of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks. Wrike will inform Customer if Wrike determines that it can no longer provide the level of protection required by such frameworks.
23. The Standard Contractual Clauses apply and take precedence over the rest of this DPA to the extent of any conflict.

Audits

24. Wrike will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, as follows:
- a. If the requested audit scope is addressed in an ISO 27001, SOC2, penetration test, or other industry-standard report issued by an independent third party auditor or security tester within the then-prior 12 months, and Wrike provides a summary of such report to Customer and confirms that there are no known material changes in the controls audited or tested, Customer agrees to accept the findings presented in the summary report in lieu of requesting an audit of the same controls covered by the report.
 - b. If the requested audit scope is not covered by such summary report(s), Wrike will provide a written description of its compliance measures for this DPA.
 - c. Wrike will provide for a further audit, provided that (i) Customer is not a competitor of Wrike and (ii) Customer reasonably believes that the information Customer received under the preceding two subparagraphs is not sufficient to demonstrate Wrike's compliance under this DPA, and (iii) Customer is exercising a legal right to an audit that cannot be satisfied using the methods mentioned above, or that is not the case but Customer is seeking a security-related audit following a Personal Data Breach. In such case:

- i. any such audit will be conducted by a third-party auditor mutually agreed upon in advance by Customer and Wrike, and the auditor agrees to written confidentiality and data security terms reasonably acceptable to Wrike, including that it will use the information it learns solely on Customer's behalf; and
 - ii. the audit may begin only after Customer and Wrike agree in advance on the audit scope, the extent of Wrike's involvement, and, in light of those things, the fees Wrike will charge Customer for the audit and any other terms that the Parties deem appropriate;
 - iii. the audit is conducted during normal business hours.
- d. Nothing herein will require Wrike to disclose or make available:
- i. any data of any other customer of Wrike;
 - ii. access to systems;
 - iii. Wrike's internal accounting or financial information;
 - iv. any trade secret of Wrike;
 - v. any information or access that, in Wrike's reasonable opinion, could (a) compromise the security of Wrike systems or premises; or (b) cause Wrike to breach its obligations under Applicable Law or applicable contracts; or
 - vi. any information sought for any reason other than the good faith fulfillment of Customer's obligations under Applicable Law to audit compliance under this DPA.
- e. Any information that Customer receives under this Section is Confidential Information of Wrike.

Limitation of Liability and Indemnification

25. As this DPA is part of the Agreement, the total aggregate liability of Wrike, including any liability for its Subprocessors' violations, under or in connection with this DPA will be subject to, and count toward, the agreed limits on liability under the Agreement. Wrike will have no liability for Personal Data Breaches or other security incidents if Wrike complies with its security obligations in this DPA or if the Personal Data Breach is otherwise attributable to (i) Customer's instructions to Wrike or other acts or omissions of Customer, (ii) Wrike's compliance with the DPA, (iii) Wrike's compliance with Customer's instructions, (iv) Customer's breach of the DPA or other aspects of the Agreement, (v) Customer's failure to use the Services in accordance with the documentation, (vi) Customer's failure to use a security or data protection option that Wrike offers, or (vii) any other situation in which Wrike is not responsible for the event giving rise to the claims, losses or damage ((i) through (vii) are collectively the "**Faultless Wrike Situations**").
26. Wrike will defend any claim, suit or governmental action brought against Customer by an unaffiliated third party arising from Wrike's breach of the DPA ("**DPA Claim**") and pay costs and damages (including reasonable attorneys' fees) finally awarded against Customer or agreed in settlement by Wrike directly attributable to such DPA Claim, provided that Customer was subscribed to Services requiring payment to Wrike in excess of \$10,000 per month, and no payment was overdue, at the time the DPA Claim first accrued. Notwithstanding any other provision of this DPA, Wrike will have no defense or indemnification obligations for a DPA Claim, and no liability of any other kind, based on claims, losses or damage arising from any of the Faultless Wrike Situations. Customer will defend any claim, suit or governmental action brought against Wrike or its affiliates by an unaffiliated third party arising from any of the Faultless Wrike Situations ("**Customer Claim**") and pay costs and damages (including reasonable attorneys' fees) finally awarded against them or agreed in settlement by Customer directly attributable to such Customer Claim.
27. The defense and indemnity and obligations apply only on condition that (i) the Party to be indemnified or defended ("**Indemnified Party**") notifies the other ("**Indemnifying Party**") in writing of the relevant claim promptly following receipt of notice, provided that failure to provide such notice promptly will relieve the Indemnifying Party of its obligations only if the delay materially prejudices defense of the matter, (ii) the Indemnifying Party has sole control of the defense and settlement (provided that the Indemnifying Party will not enter into a settlement that imposes non-monetary relief beyond discontinuation of provision or use of the Services between the Parties without the Indemnified Party's written consent, which shall not be unreasonably withheld), (iii) the Indemnified Party provides the Indemnifying Party with all information and communications received from the claimant regarding the claim, and (iv) the Indemnified Party provides reasonable assistance to the Indemnifying Party when requested. The Indemnified Party will have the right to participate in the defense with counsel of its own choosing at its expense provided that such representation does not interfere with the Indemnifying Party's right to control the defense.

Return or Destruction

28. Wrike will, at Customer's choice, return to Customer and/or destroy all Personal Data after the termination or expiration of Customer's subscription to the relevant Services, except to the extent Applicable Law requires storage of the Personal Data, within (a) 30 days for Personal Data in Wrike's production environment and (b) 187 days for Personal Data from files created for security, backup, or business continuity purposes. If Wrike has not received Customer's election within 30 days of such termination or expiration, Wrike may assume that Customer has selected deletion and reserves the right to delete Personal Data consistent with the foregoing. Certification of deletion under Clause 12 of the Standard Contractual Clauses (if they apply) will be provided only on written request.
29. If Customer requires earlier deletion of such Personal Data, and such deletion is commercially feasible, Customer must first pay Wrike's reasonable fees for such deletion, which may include costs for business interruptions associated with such a request.

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.	Company: <u>Universität Siegen</u>
By: [Redacted]	By: [Redacted]
Name: [Redacted]	Name: _____
Title: [Redacted]	Title: _____
Date: July 31, 2020	Date: <u>15.12.2020</u>
Address: 70 North Second Street San Jose, CA 95113 USA	Address: [Redacted]
Notice Copy: legal@team.wrike.com	Notice Copy: _____
Security Point of Contact: security@team.wrike.com	Security Point of Contact: _____
Secondary Security Point of Contact: privacy@team.wrike.com	Secondary Security Point of Contact (if any): _____
	Data Protection Officer (if any): _____
	GDPR Representative in the EU (if any): _____

Annex A

**Commission Decision C(2010)593
Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Universität Siegen
Address: Adolf-Reichwein-Str. 2a, 57076 Siegen, Germany
Tel.: (+49) 271 1740-0
fax:
e-mail:

Other information needed to identify the organisation: None

(the data exporter)

And

Name of the data importing organisation: Wrike, Inc.
Address: 70N Second Street, San Jose, CA, 95113, USA
Tel.: 877-779-7453
e-mail: privacy@team.wrike.com

Other information needed to identify the organisation: None

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses³. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter: [Redacted]
Name (written out in full): [Redacted]
Position: [Redacted]
Address: [Redacted]
Other information necessary in order for the contract to be binding (if any): None

(stamp of organisation)

Signature: [Redacted]

On behalf of the data importer:
Name (written out in full): [Redacted]
Position: [Redacted]
Address: Wrike, Inc., 70N Second Street, San Jose, CA, 95113, USA
Other information necessary in order for the contract to be binding (if any): None

(stamp of organisation)

Signature: [Redacted]



³ Decision. This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): The data exporter is Customer, a user of the Services.

Data importer

The data importer is (please specify briefly activities relevant to the transfer): Wrike, Inc., provider of the Services.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): Depending on Customer's usage, this could include the exporter's personnel, as well as individuals in other categories, such as exporter's customers, service providers, business partners, affiliates and users of exporter's website or online service.

Categories of data

The personal data transferred concern the following categories of data (please specify): The open nature of the Services does not impose a technical restriction on the categories of data Customer may provide. The Personal Data Processed by Wrike may thus include name, email address, telephone and fax number, title, and other information.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): None anticipated, but the open nature of the Services does not impose a technical restriction on the categories of data Customer may provide. The Personal Data Processed by Wrike may thus include all special categories of data.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): The subject matter, nature and purpose of the processing are Wrike's provision of the Services to Customer. This involves storing personal data, making it available to Customer for modification and transmission, and deleting personal data. The processing takes place from the commencement of the Agreement until deletion of all Personal Data by Wrike in accordance with the DPA.

DATA EXPORTER

Name: Universität Siegen

Authorised Signature 

DATA IMPORTER

Name: Wrike, Inc.

Authorised Signature 

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Wrike's then-current Information Security Addendum, designed to comply with industry-standard ISO 27001 and SOC2 organizational controls and applicable law, can be found at <https://learn.wrike.com/enterprise-winfosec/>.

Annex B
Security Measures

Wrike's then-current Information Security Addendum, designed to comply with industry-standard ISO 27001 and SOC2 organizational controls and applicable law, can be found at <https://learn.wrike.com/enterprise-winfosec/>.

[End of Document]