Atlassian Data Processing Addendum

This Data Processing Addendum ("**DPA**") amends the terms and forms part of the Agreement (defined below) by and between you ("**Customer**") and the applicable Atlassian entity from which you are purchasing Cloud Products ("**Atlassian**") and shall be effective on the later of (i) the effective date of the Agreement; or (ii) the date both parties execute this DPA in accordance with Section 1 below ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Instructions and Effectiveness

1.1. This DPA has been pre-signed on behalf of Atlassian. To enter into this DPA, Customer must:

(a) be a customer of the Cloud Products;

(b) complete the signature block below by signing and providing all relevant information; and

(c) submit the completed and signed DPA to Atlassian.

1.2. This DPA will only be effective (as of the Effective Date) if executed and submitted to Atlassian accurately and in full accordance with Section 1. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

1.3. Customer signatory represents to Atlassian that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

1.4. Notwithstanding expiry or termination of the Agreement, this DPA and any Standard Contractual Clauses (if applicable) will remain in effect until, and will terminate automatically upon, deletion by Atlassian of all personal data covered by this DPA, in accordance with this DPA.

2. Data Protection

2.1. *Definitions:* In this DPA, the following terms shall have the following meanings:

(a) "**Agreement**" means the contract in place between Customer and in connection with the purchase of Cloud Products by Customer;

(b) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in European Data Protection Law;

(c) "**Applicable Data Protection Law**" means US Data Protection Law and European Data Protection Law that are applicable to the processing of Customer Personal Data under this DPA;

(d) "**Customer Personal Data**" means any personal data provided by (or on behalf of) Customer to Atlassian in connection with the Services, all as more particularly described in this DPA.

(e) "**EEA**" means the European Economic Area;

(f) **"End Users"** means an individual you permit or invite to use the Cloud Products. For the avoidance of doubt: (a) individuals invited by your End Users, (b) individuals under managed accounts, and (c) individuals interacting with a Cloud Product as your customer are also considered End Users.

(g) "**European Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act ("**Swiss DPA**").

(h) "**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

(i) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

(j) "**Standard Contractual Clauses**" means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("**UK SCCs**"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (the "**Swiss SCCs**").

(k) "**Security Incident**" means any confirmed breach of security that leads to the accidental, unauthorized or unlawful destruction, loss, alteration, disclosure of or access to Customer Personal Data processed by Atlassian and/or its Sub-processors in connection with the provision of the Service. "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(l) "**Services**" means the provision of the Cloud Products by Atlassian to Customer pursuant to the Agreement.

(m) "**special categories of data**" means any Customer Personal Data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) that is genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, and (iii) relating to criminal convictions and offences.

(n) "**Sub-processor**" means any processor engaged by Atlassian to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data. Sub-processors may include Atlassian's affiliates or other third parties.

(o) "**U.S. Data Protection Law**" means all data protection or privacy laws and regulations applicable to the Customer Personal Data in question in force within the United States, including the California Consumer Privacy Act (as may be amended from time to time) (the "**CCPA**"), and any rules or regulations implementing the foregoing.

2.2. *Relationship of the parties*: Where Applicable Data Protection Law provides for the roles of "controller," "processor," and "subprocessor":

(a) Where Customer is a controller of the personal data covered by this DPA, Atlassian shall be a processor processing personal data on behalf of the Customer and this DPA shall apply accordingly;

(b) Where Customer is a processor of the personal data covered by this DPA, Atlassian shall be a Sub-processor of the personal data and this DPA shall apply accordingly; and

(c) Where and to the extent Atlassian processes personal data as a controller, Atlassian will process such personal data in compliance with Applicable Data Protection Laws and only Sections 2.6 and 3.1 of this DPA, to the extent applicable.

2.3. *Description of Processing*: A description of the processing of personal data related to the Services, as applicable, is set out in Exhibit A. The parties acknowledge and agree that the description of processing can be updated by Atlassian from time to time to reflect new products, features or functionality comprised within the Services. Atlassian will update relevant documentation to reflect such changes.

2.4. *Customer Processing of Personal Data*. Customer agrees that (i) it will comply with its obligations under Applicable Data Protection Law in its processing of Customer Personal Data and any processing instructions it issues to Atlassian; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Laws for Atlassian to process personal data (including but not limited to any special categories of data) and provide the Services pursuant to the Agreement (including this DPA).

2.5. *Purpose limitation:* Atlassian shall process the Customer Personal Data as a processor, as necessary to perform its obligations under the Agreement and strictly in accordance with the documented lawful instructions of Customer (as set forth in the Agreement, or in this DPA, or as directed by you through the Cloud Products) (the "**Permitted Purpose**"). Atlassian shall not retain, use, disclose or otherwise process the Customer Personal Data for any purpose other than the Permitted Purpose except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law, and shall not "sell" the Customer Personal Data within the meaning of the CCPA or otherwise. Atlassian shall promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law.

2.6. *Restricted transfers:* The parties agree that when the transfer of Customer Personal Data from Customer (as "data exporter") to Atlassian (as "data importer") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, it shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA, as follows:

(a) In relation to transfers of Customer Personal Data protected by the EU GDPR and processed in accordance with Sections 2.2(a) and 2.2(b) of this DPA, the EU SCCs shall apply, completed as follows:

i. Module Two or Module Three will apply (as applicable);

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 2.10 of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

vii. Annex I of the EU SCCs shall be deemed completed with the information set out in EXHIBIT A to this DPA, as applicable; and

viii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in EXHIBIT B to this DPA;

(b) In relation to transfers of Customer Personal Data protected by the EU GDPR and is processed in accordance with Section 2.2(c) of this DPA, the EU SCCs shall apply, completed as follows:

i. Module One will apply;

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 11, the optional language will not apply;

iv. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

v. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

vi. Annex I of the EU SCCs shall be deemed completed with the information set out in EXHIBIT A to this DPA, as applicable; and

vii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in EXHIBIT B to this DPA;

(c) In relation to transfers of Customer Personal Data protected by the UK GDPR, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:

i. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;

ii. references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;

iii. Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts",

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the UK GDPR in which case the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in EXHIBITS A and B of this DPA (as applicable);

(d) In relation to transfers of Customer Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:

i. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

ii. references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and

iii. references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland,

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss DPA in which case the Swiss SCCS shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in EXHIBITS Aand B to this DPA (as applicable);

(e) It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict;

(f) Although Atlassian does not rely on the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("Privacy Shield") as a legal basis for transfers of Customer Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as Atlassian, Inc. and its covered entities are self-certified to the Privacy Shield Atlassian shall continue to process Customer Data in accordance with the Privacy Shield Principles. Atlassian will promptly notify Customer if it makes a determination that Atlassian can no longer meet its obligations under the Privacy Shield Principles; and

(g) If Atlassian adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to Applicable Data Protection Laws) for the transfer of Customer Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Customer Data is transferred).

2.7. *Confidentiality of processing:* Atlassian shall ensure that any person that it authorises to process Customer Personal Data (including Atlassian's staff, agents and Sub-processors) (an "**Authorised Person**") shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process Customer Personal Data who is not under such a duty of confidentiality.

2.8. *Security:* Atlassian and, to the extent required under the Agreement, Customer shall implement appropriate technical and organisational measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with Atlassian's security standards described in Exhibit B ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Atlassian may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

2.9. *Subprocessing:* Customer agrees that Atlassian may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by Atlassian and authorized by Customer are listed at https://www.atlassian.com/legal/sub-processors. Atlassian will: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Laws (and in substance, to the same standard provided by this DPA); and (ii) remain responsible to Customer for the performance of such Sub-processor's data protection obligations under such terms.

2.10. Changes to Sub-processors: Atlassian shall (i) make available an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer if it adds any new Sub-processors at least fourteen (14) days' prior to allowing such Sub-processor to process Customer Personal Data. Customer must subscribe to receive notice of updates to the list of Sub-processors, using the link in Section 2.9. Customer may object in writing to Atlassian's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the Agreement (including this DPA) for convenience.

2.11. *Cooperation and data subjects' rights:*

(a) Atlassian shall provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party, in each case in respect of Customer Personal Data that Atlassian processes on Customer's behalf;

(b) In the event that any request, correspondence, enquiry or complaint (referred to under paragraph (a) above) is made directly to Atlassian, Atlassian acting as a processor shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so, and instead, after being notified by Atlassian, Customer shall respond. If Atlassian is legally required to respond to such a request, Atlassian will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so; and

(c) To the extent Atlassian is required under Applicable Data Protection Law, Atlassian shall (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

2.12. *Security incidents:* Upon becoming aware of a Security Incident, Atlassian shall inform Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer to allow Customer to fulfil its data breach reporting obligations under Applicable Data Protection Law. Customer

shall further take reasonable steps to contain, investigate, and mitigate the effects of the Security Incident. Atlassian's notification of or response to a Security Incident in accordance with this section 2.12 will not be construed as an acknowledgment by Atlassian of any fault or liability with respect to the Security Incident.

2.13. *Deletion or return of Data:* Upon written request from Customer, Atlassian shall anonymize, delete, or return to Customer all Customer Personal Data (including copies) in its possession or control, in compliance with the procedures and retention periods outlined in the DPA, Cloud Product Specific Terms or Trust Center; this requirement shall not apply to the extent Atlassian is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Atlassian shall securely isolate and protect from any further processing, except to the extent required by applicable law.

2.14. *Audit:*

(a) Customer acknowledges that Atlassian is regularly audited by independent third-party auditors and/or internal auditors including as may be described from time to time at https://www.atlassian.com/trust/compliance. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Atlassian, Atlassian shall:

i. supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Customer, so Customer can verify Atlassian's compliance with the audit standards against which it has been assessed, and this DPA; and

ii. provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security and audit questionnaires, that are necessary to confirm Atlassian's compliance with this DPA, provided that Customer shall not exercise this right more than once per calendar year.

(b) Only to the extent Customer cannot reasonably satisfy Atlassian's compliance with this DPA through the exercise of its rights under Section 2.14(a) above, where required by Applicable Data Protection Law or the Standard Contractual Clauses, Customer and its authorized representatives may conduct audits (including inspections) during the term of the Agreement to establish Atlassian's compliance with the terms of this DPA, on the condition that Customer and its authorized representatives have entered into an applicable non-disclosure agreement with Atlassian. Notwithstanding the foregoing, any audit (or inspection) must be conducted during Atlassian's regular business hours, with reasonable advance notice (which shall not be less than 45 calendar days) and subject to reasonable confidentiality procedures. Such audit (or inspection) shall not require Atlassian to disclose to Customer or its authorized representatives, or to allow Customer or its authorized representatives to access:

i. any data or information of any other Atlassian customer (or such customer's End Users);

ii. any Atlassian internal accounting or financial information;

iii. any Atlassian trade secret;

iv. any information that, in our reasonable opinion could: (1) compromise the security of our systems or premises; or (2) cause us to breach our obligations under Applicable Data Protection Law or our security, confidentiality and or privacy obligations to any other Atlassian customer or any third party; or

v. any information that Customer or its authorized representatives seek to access for any reason other than the good faith fulfilment of Customer's obligations under the Applicable Data Protection Law and Atlassian's compliance with the terms of this DPA.

(c) An audit or inspection permitted in compliance with Section 2.14(b) shall be limited to once per calendar year, unless (1) Atlassian has experienced a Security Incident within the prior twelve (12) months which has impacted Customer Personal Data; or (2) Customer is able to evidence an incidence of Atlassian's material noncompliance with this DPA.

2.15. *Law enforcement*: If a law enforcement agency sends Atlassian a demand for Customer Personal Data (e.g., a subpoena or court order), Atlassian will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Atlassian may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then Atlassian will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Atlassian is legally permitted to do so.

3. Miscellaneous

3.1. Customer acknowledges and agrees that as part of providing the Cloud Products and services, Atlassian has the right to use data relating to or obtained in connection with the operation, support or use of the Cloud Products for its legitimate internal business purposes, such as to support billing processes, to administer the Cloud Products, to improve, benchmark, and develop Atlassian products and services, to comply with applicable laws (including law enforcement requests), to ensure the security of the Cloud Products and to prevent fraud or mitigate risk. To the extent any such data is personal data, Atlassian warrants and agrees that:

(a) it will process such personal data in compliance with Applicable Data Protection Law and only for the purposes that are compatible with those described in this Section 3.1; and

(b) it will not use such personal data for any other purpose or disclose it externally unless it has first aggregated and anonymised the data so it does not identify the Customer or any other person or entity.

3.2. Through use of the Cloud Products, as further described in the Agreement, Customer or Customer's End Users, as applicable, may elect to grant third parties visibility to data or content (which may include Customer Personal Data). Customer understands that user

profile information for the Cloud Products may be publicly visible. Nothing in this DPA prohibits Atlassian from making Customer's data or content (which may include personal data) visible to third parties consistent with this paragraph, as instructed by Customer or Customer's End Users through the Cloud Products.

4. Relationship with the Agreement:

4.1. The parties agree that this DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.

4.2. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data. If there if any conflict between the Standard Contractual Clauses and the Agreement (including this DPA), the Standard Contractual Clauses shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data.

4.3. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

4.4. Any claims against Atlassian or its affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the Atlassian entity that is a party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

4.5. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

4.6. This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically upon deletion by Atlassian of the personal data covered by this DPA, in accordance with Section 2.13 of this DPA.

CUSTOMER

Customer name (Required): _____

Signature (Required): _____

Name (Required): _____

Title (Optional): _____

Date (Required): _____

EU Representative (Required only where applicable): _____

Contact details: _____

Data Protection Officer (Required only where applicable): _____

Contact details: _____

ATLASSIAN

Notwithstanding the signatures below of any other Atlassian Entity, an Atlassian Entity is not a party to this Addendum unless they are a party to the Agreement for the provision of the Cloud Products to you. Where the Cloud Products are provided under an Agreement with Atlassian Pty Ltd, Atlassian, Inc. is also a party tothis Addendum.

Data Protection Point of Contact: Kelly Gertridge

Contact Details: dataprotection@atlassian.com

Atlassian PTY Ltd.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022
Atlassian, Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022

Trello Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022
Dogwood Labs, Inc. (dba Statuspage.io)	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022
OpsGenie, Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022
Agile Craft LLC	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022
Halp Inc.	Signature: Kelly Gertridge Name: Kelly Gertridge Title: Head of Privacy Date: 1/05/2022

EXHIBIT A
Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: Customer	Name: Atlassian
Address / Email Address: As provided for in the DPA	Address / Email Address: As provided for in the DPA
Contact Person's Name, position and contact details: As provided for in the DPA	Contact Person's Name, position and contact details: As provided for in the DPA
Activities relevant to the transfer: See Annex 1(B) below	Activities relevant to the transfer: See Annex 1(B) below
Role: See Annex 1(B)	Role: See Annex 1(B)

Annex 1(B) Description of Processing / Transfer

The parties acknowledge that Atlassian's processing of personal data will include all personal data submitted or uploaded to the Services by Customer from time to time, for the purpose of, or otherwise in connection with, Atlassian providing the Services to Customer. Set out below are descriptions of the processing/transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or may be supplemented pursuant to Section 2.3 of the DPA.

Atlassian cloud account profile (Identity)	
Categories of data subjects	Customers, customers' employees, customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	  ○ About me
	• Personal Identification
	• Employment Information, including:
	  ○ Job title / role
	  ○ Office / location
	  ○ Company/Organization

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous

Nature of the processing	Providing the products and services, including: • To maintain and display user profiles during collaboration, authenticate users, and manage access control and user permissions.
Purpose of the data transfer	Providing the products and services, including: • To allow collaboration and maintain proper access controls and user permissions.
Duration of processing	Data will be deleted 15 days (for evaluation sites) or 60 days (for paid subscription sites) after a customer been unsubscribed due to missed payment for an Atlassian product subscription or if a customer cancels their Atlassian product subscription. For more information see https://support.atlassian.com/security-and-access-policies/docs/track-storage-and-move-data-across-products/
Jira Cloud	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	  ○ About me
	• Personal Identification, including:
	  ○ Device Information - Mobile
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Import/export issues and records • Track projects • Search content • Create and edit pages • Save and store files • Display profiles • Provide user alerts and messages
Purpose of the data transfer	Providing the products and services, including: • User and team communication • File sharing • Media management • Search • Content publishing • Third-party integration

Duration of processing	Upon termination of service, customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the customer's current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.
Confluence Cloud	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Company/Organization
	  ○ Full Name
	  ○ Email address
	• Personal Identification, including:
	  ○ Device Information - Mobile
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Import/export pages and records • Track projects • Search content • Create and edit pages • Save and store files • Display profiles • Provide user alerts and messages
Purpose of the data transfer	Providing the products and services, including: • User and team communication • File sharing • Media management • Search • Content publishing • Third-party integration
Duration of processing	Upon termination of service, customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the customer's current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the customer's current subscription period. Upon

	deletion, an archive of the data is kept for an additional 30 days.
Jira Service Management / Jira Work Management (Also see section for Ops Genie, which is integrated into JSM and JWM)	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Company/Organization
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification, including:
	  ○ IP Address
	  ○ Language Setting
	  ○ Location/ Region/ City
	  ○ Phone numbers
	  ○ Screen name/ Handle/ Nickname
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Import/export issues and records • Tracking activity • Search content • Create and edit pages and content • Save and store files • Display profiles • Support systems / admin controls • Provide user alerts and messages
Purpose of the data transfer	Providing the products and services, including: • User and team communication • Account and login management • File sharing • Media management • Search • Content publishing • Third party integration
Duration of processing	Upon termination of service, customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the customer's current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the customer's current subscription period. Upon

	deletion, an archive of the data is kept for an additional 30 days.
Bitbucket Cloud	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Company/Organization
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	  ○ Bitbucket ID
	• Personal Identification, including:
	  ○ IP Address
	  ○ Language Setting
	  ○ Location/ Region/ City
	  ○ Phone numbers
	  ○ Screen name/ Handle/ Nickname
	  ○ Job title / role
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Login/ Sign up • Export Repository • Debugging • Password Management • Source Code Repositories • Import/Exports • Tracking Activity • Search Query/ Content • Create/edit pages • Save/ Store files • Display profiles • Support Systems/ Admin controls • Alerts/ Messages
Purpose of the data transfer	Providing the products and services, including: • User/Team Communication • File Sharing • Media Management • Support/ Feedback • Search • Content Publishing • Account/ Login Management • Product Performance

	• Security • Third party integration
Duration of processing	On termination of a Bitbucket Cloud account, and at the request of the customer, customer data will be removed from the live production database. The team's data will remain in encrypted Bitbucket Cloud database backups until those backups fall out of the 35-day backup retention window and are destroyed in accordance with Bitbucket Cloud's data retention policy. In the event a database restore is necessary within 35 days of a requested data deletion, the Bitbucket Cloud operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.
Trello	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Company/Organization
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification, including:
	  ○ IP Address
	  ○ Cookie Information
	  ○ Device Information - Mobile
	  ○ Language Setting
	  ○ Location/ Region/ City
	  ○ Phone numbers
	  ○ Screen name/ Handle/ Nickname
	  ○ Job title / role
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Import/export cards and records • Tracking Activity • Search Query/ Content • Create/edit pages & content • Save/ Store files • Display profiles • Support Systems/ Admin controls • Alerts

	• Support Systems/ Admin controls
Purpose of the data transfer	Providing the products and services, including: • User/Team Communication • File Sharing • Media Management • Support/ Feedback • Search • Content Publishing • Account/ Login Management • 3rd Party Integration
Duration of processing	On termination of a Trello Enterprise contract, and at the request of the customer, the data belonging to the Enterprise teams will be completely removed from the live production database and all file attachments uploaded directly to Trello will be removed within 30 days. The team's data will remain in encrypted Trello database backups until those backups fall out of the 90-day backup retention window and are destroyed in accordance with Trello's data retention policy. In the event a database restore is necessary within 90 days of a requested data deletion, the Trello operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.
Opsgenie	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Company/Organization
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification, including:
	  ○ IP Address
	  ○ Cookie Information
	  ○ Device Information - Mobile
	  ○ Language Setting
	  ○ Location/ Region/ City
	  ○ Phone numbers
	  ○ Screen name/ Handle/ Nickname
	  ○ Job title / role
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous

Nature of the processing	Providing the products and services, including: • Import/export records • Tracking Activity • Search Query/ Content • Create/edit pages & content • Save/ Store files • Display profiles • Support Systems/ Admin controls • Alerts • Support Systems/ Admin controls
Purpose of the data transfer	Providing the products and services, including: • User/Team Communication • Account/ Login Management • Third Party Integration
Duration of processing	When a configuration item, user, or alert, incident is deleted from Opsgenie, the entity and child data will be deleted by Opsgenie. When a user is deleted from Opsgenie, Audit Logs (Alert Log - Incident Timeline) will still have audit records like "Email notification sent to x@y.com", this is important as part of Incident audit. Customers can delete Alerts & Incident, Alert logs & Incident Timeline will be deleted. Customer Logs visible on Logs page are immutable, has a retention of 1 year. Customers can delete data from web applications manually or automatically by using Opsgenie rest api. When paid subscription ends customers shall contact Customer Support so that all data of customers can be deleted. Legal & Security Auditing reasons: Customer Logs, Data Backup & System Log Archives will be stored as an archive for 1 year, regardless of customer data is fully deleted or not. Archives can not be accessed directly by customers, restricted to Opsgenie authorized employees.
Statuspage	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Atlassian identifier associated with a user account
	  ○ About Me
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification
	• Employment Information, including:
	  ○ Company/Organization
	• Personal data in User Generated Content
	• Browsing information on Admin settings

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Login/ Sign up • Import/export records • Tracking Activity • Search Query/ Content • Create/edit content (incident communication) • Save/ Store files • Display profiles • Support Systems/ Admin controls • Notifications
Purpose of the data transfer	Providing the products and services, including: • Incident communication • Scheduled maintenances • Support/ Feedback • Content Publishing • Account/ Login Management • Third party integration
Duration of processing	On termination of a Statuspage account, and at the request of the customer, customer data will be removed from the live production database. The customer data will remain in encrypted Statuspage database backups until those backups fall out of the 30-day backup retention window and are destroyed in accordance with Atlassian's data retention policy. In the event that a database restore is necessary within 30 days of a requested data deletion, the Statuspage operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.
Jira Align	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ Jira Align ID
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification, including::
	  ○ Screen name/ Handle/ Nickname
	  ○ Language Setting
	  ○ Location/ Region/ City
	• Employment Information, including:
	  ○ Job Title/ Role
	• Browsing information on Admin settings
	• Contact Information
	• Personal data in User Generated Content

Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)

Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Import/export records • Tracking Activity • Search Query/ Content • Create/edit pages • Save/ Store files • Display profiles • Support Systems/ Admin controls • Alerts/ Messages • Data Warehouse Sync • Provide Business intelligence for Customer
Purpose of the data transfer	Providing the products and services, including: • User/Team Communication • File Sharing • File Storage • Media Management • Support/ Feedback • Search • Content Publishing • Account/ Login Management • Business Analytics • Third party integration
Duration of processing	On termination of a Jira Align Enterprise contract, and at the request of the customer, the database will be dropped from the live production database. This will be done within the support team service level agreement. The customer data will remain in encrypted Jira Align database backups until those backups fall out of the 35-day backup retention window and are destroyed in accordance with Atlassian's data retention policy. In the event a database restore is necessary within 35 days of a requested data deletion, the Jira Align operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.
Halp	
Categories of data subjects	Customers, customers' employees, and customers' collaborators

Categories of personal data transferred	• User Account Information, including:
	  ○ User ID
	  ○ Avatar Image
	  ○ Avatar URL
	  ○ Full Name
	  ○ Email address
	  ○ Time zone
	• Personal Identification, including:
	  ○ Screen name/ Handle/ Nickname
	  ○ Phone number
	  ○ IP Address
	• Employment Information, including:
	  ○ Job Title/ Role
	  ○ Halp role
	  ○ Zendesk User ID*

	○ Zendesk User Role* • Browsing information on Admin settings • Personal data in User Generated Content *only if customers integrate with Zendesk
Controller/ Processor roles	Controller (Customer) to Processor (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Use email address to map identities. in Jira/ Slack (resolving identities) • Display user profiles • Logging in/Authentication • Create & update tickets • Sync data between different platforms (e.g., Sync data primarily from Jira/ Zendesk/ MS Teams) • Create tickets from email/ web client/ Slack • Provide user alerts and messages
Purpose of the data transfer	Providing the products and services, including: • User/Team Communication • File Sharing • Content management • Support/ Feedback • Account/ Login Management • Business Analytics • Third party integration
Duration of processing	At the request of the customer, the data belonging to the customer will be completely removed from the live production database and all file attachments uploaded directly to Halp will be removed within 30 days. The team's data will remain in encrypted Halp database backups until those backups fall out of the 90-day backup retention window and are destroyed in accordance with Halp's data retention policy. In the event that a database restore is necessary within 90 days of a requested data deletion, the Halp operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored. In the event that a database restore is necessary within 35 days of a requested data deletion, the Jira Align operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.
Atlassian business operations & analytics ("Usage Data")	
Categories of data subjects	Customers, customers' employees, and customers' collaborators
Categories of personal data transferred	• User Account Information, including: ○ Atlassian Account ID ○ Bitbucket Account ID ○ Opsgenie Account ID ○ Statuspage Account ID ○ Trello Account ID ○ Atlassian Cloud ID / Site ID / Tenant ID

	○ Segment Anonymous ID • Personal Identification, including: ○ IP address ○ Cookie information ○ Device information • Browser information • Metadata, including: ○ Event Name (i.e. what action the user performed) ○ Event Timestamp ○ Page URL ○ Referring URL
Controller/ Processor roles	Controller (Customer) to Controller (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Storing records of user actions performed within products and websites, including support sites and marketing sites
Purpose of the data transfer	Providing the products and services, including: • To provide and administer the products, support, and services, including to calculate usage-based billing • To facilitate security, fraud prevention, performance monitoring, business continuity, and disaster recovery • To comply with legal and financial reporting obligations • To derive insights in order to develop and improve the products, support, and services • To derive insights in order to support business development
Duration of processing	Pseudonymized records of user actions performed within products and websites are retained for 2.5 years in an online and readily accessible format. Aggregated and anonymized records of some key user actions performed within products and websites are retained permanently.
Atlassian Support	
Categories of data subjects	Customers, customers' employees, and customers' collaborators
Categories of personal data transferred	• User Account Information, including: • Atlassian account ID • About me • Address • Avatar Image • Avatar URL • Full Name • Email address • Time zone • SEN (Support Entitlement Number) • Personal Identification, including: • IP Address • Device Information – Mobile • Language setting

	• Location/region/city • Phone number • Screen name/ Handle/ Nickname • Employment Information, including: • Company/organization • Job title • Office location • Contact Information • Education & Skills • Financial Information • Personal data in User Generated Content
Controller/ Processor roles	Controller (Customer) to Processor (Atlassian) Controller (Customer) to Controller (Atlassian)
Sensitive data transferred?	None
Frequency of the transfer	Continuous
Nature of the processing	Providing the products and services, including: • Engage and respond to customer support questions • Marketing activities • Sales activities • Authentication/ System admin • Financial, training and certification • Collect/Manage sales • Analyse business metadata
Purpose of the data transfer	Providing the products and services, including: • Support/ Feedback • Marketing/ Engagement • Account/ Login Management • Business Analytics • Search
Duration of processing	Production customer data is replicated only to a single staging (pre-production) environment. This staging environment is refreshed every 30 days. Support cases are maintained for 5 years after closure. Files attached to support cases are deleted 60 days after case closure.

Annex 1(C): Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the New EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to the processing of personal data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to the processing of personal data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT B

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymisation and encryption of personal data	See https://www.atlassian.com/trust/security/security-practices#encryption-of-data; and https://www.atlassian.com/trust/security/security-practices#key-management
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	See https://www.atlassian.com/trust/security/security-practices#controlling-access-to-customer-data; https://www.atlassian.com/trust/security/security-practices#service-availability; https://www.atlassian.com/trust/security/security-practices#backups; and https://www.atlassian.com/trust/security/security-practices#tenant-separation
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	See https://www.atlassian.com/trust/security/security-practices#business-continuity-and-disaster-recovery-management
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	See https://www.atlassian.com/trust/security/security-practices#internal-and-external-audit

Measures for user identification and authorisation	Atlassian cloud users can authenticate using username and password, or external IdPs (incl. via SAML, Google, Microsoft and Apple). All credentials are hosted in the application database, which is encrypted at REST. Passwords are hashed using a secure hashing algorithm. Administrators are able to configure and enforce password complexity requirements for managed accounts via Access: https://support.atlassian.com/security-and-access-policies/docs/manage-your-password-policy/. Administrators are also able to enforce SSO via Access.
Measures for the protection of data during transmission	See https://www.atlassian.com/trust/security/security-practices#encryption-of-data
Measures for the protection of data during storage	See https://www.atlassian.com/trust/security/security-practices#data-centers; and https://www.atlassian.com/trust/security/security-practices#key-management
Measures for ensuring physical security of locations at which personal data are processed	See https://www.atlassian.com/trust/security/security-practices#physical-security
Measures for ensuring events logging	See https://www.atlassian.com/trust/security/security-practices#making-use-of-logs; and https://www.atlassian.com/trust/security/security-practices#security-detections-program
Measures for ensuring system configuration, including default configuration	See https://www.atlassian.com/trust/security/security-practices#infrastructure; and https://www.atlassian.com/trust/security/security-practices#managing-configurations-in-systems
Measures for internal IT and IT security governance and management	See https://www.atlassian.com/trust/security/security-management-program; and https://www.atlassian.com/trust/compliance/risk-management-program

Measures for certification/assurance of processes and products	See https://www.atlassian.com/trust/compliance; and https://www.atlassian.com/trust/compliance/compliance-faq
Measures for ensuring data minimisation	See "What information we collect about you" section of https://www.atlassian.com/legal/privacy-policy#what-information-we-collect-about-you
Measures for ensuring data quality	Users may update their data through profile settings https://support.atlassian.com/atlassian-account/docs/update-your-profile-and-visibility-settings/
Measures for ensuring limited data retention	Atlassian maintains a Data Retention and Destruction Standard, which designates how long we need to maintain data of different types. The Data Retention & Disposal Standard is guided by the following principles: • Records should be maintained as long as they serve a business purpose. • Records that serve a business purpose, or which Atlassian has a legal, regulatory, contractual or other duty to retain, shall be retained. • Records that no longer serve a business purpose, and for which Atlassian has no duty to retain, should be disposed. Copies or duplicates of such data should also be disposed. To the extent Atlassian has a duty to retain a specified number of copies of a Record, such number of copies should be retained. • Atlassian's practices implementing this Standard may vary across departments, systems and media, and will of necessity evolve over time. These practices will be reviewed under our company-wide policy review practices.
Measures for ensuring accountability	See https://www.atlassian.com/trust/compliance; and https://www.atlassian.com/trust/compliance/compliance-faq
Measures for allowing data portability and ensuring erasure	See "Managing Individual privacy rights" on https://www.atlassian.com/hu/trust/privacy/business-data-privacy; and "Privacy requests" on https://www.atlassian.com/hu/trust/privacy/personal-data-privacy