Data Processing Agreement

CertKit

This Agreement was last modified on April 21, 2026.

This Data Processing Agreement (the "DPA") is entered into by and between TrackJS LLC, a Minnesota limited liability company with offices at 2112 Broadway St NE STE 225 PMB 25, Minneapolis, MN 55413-3081 USA ("TrackJS", "CertKit", "we", or "us") and the entity you represent (the "Customer" or "you").

You have entered into one or more agreements with CertKit, including our Terms of Service, https://www.certkit.io/terms, and Privacy Policy, https://www.certkit.io/privacy, (collectively, as amended, the "Agreement") that govern the use of the CertKit automated TLS certificate management service as described at https://www.certkit.io/ (the "Service"). This DPA will amend the Agreement to reflect the parties' rights and responsibilities with respect to the processing and security of Personal Data and Customer Data (as defined below) under the Agreement. If you are accepting this DPA in your capacity as an employee, consultant, or agent of the Customer, you represent and warrant that you have the authority to bind the Customer to this DPA.

Executing the Agreement

This DPA consists of both the definitions and provisions of this agreement, the Standard Contractual Clauses, and Annexes I, II, III, and IV. The DPA has been pre-signed on behalf of CertKit as the Data Importer.

To execute the DPA, Customer must (a) complete and sign the DPA's signature page, and, if Customer provides Personal Data subject to the GDPR to CertKit, and (b) complete and sign the Standard Contractual Clauses Data Processing Description in Annex I.

You must send the completed and signed DPA to CertKit by email at hello@certkit.io. Upon receipt of the validly-completed DPA by CertKit at this address, the DPA shall be in effect and legally bind the parties.

1. Definitions

The terms used in this DPA shall have the meanings set forth in this DPA. Terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

"Applicable Data Protection Law" shall mean all applicable international, national, federal, state, provincial, and local laws, rules, regulations, directives, and governmental requirements currently in effect, or as they become effective, relating in any way to the privacy, confidentiality,

or security of the Processing of Personal Data (defined below), including but not limited to the General Data Protection 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 (the "GDPR"), the e-Privacy Directive 2002/58/EC, the ePrivacy Regulation 2017/003 (once it takes effect), the California Consumer Privacy Act of 2018, Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code ("CCPA") and any equivalent or similar laws, rules, regulations, directives, and governmental requirements in applicable jurisdictions, and any laws implementing, replacing or supplementing any of them, as amended, consolidated, re-enacted or replaced from time to time.

"Business" and "Service Provider" shall have the meanings set forth in the CCPA.

"Data Controller", "Data Processor", "Data Subject", and "Processing" shall have the meanings given in Applicable Data Protection Law.

"Personal Data" shall mean any "personal data" or "personal information" (as those terms are defined in Applicable Data Protection Law) contained within Customer Data.

"Customer Data" means any data you submit to, store on, or send to CertKit via the Service.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data on systems that are managed and controlled by CertKit. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including, without limitation, pings, port scans, denial of service attacks, network attacks on firewall or networked systems, or unsuccessful login attempts.

"Notification Email Address" means the email address(es) of users that you designate to receive notifications when you create an account to use the Service. You agree that you are solely responsible for ensuring that your Notification Email Address is current and valid at all times.

"Sub-processor" means a third party that we use to process Customer Data in order to provide parts of the Service and/or related technical support.

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to processors approved by the European Commission as set forth in Appendix 1 and as may be amended, superseded, or replaced from time to time.

2. Data Processing

2.1 Scope of this DPA

While providing the Services to Customer pursuant to the Agreement, CertKit may Process Personal Data on behalf of Customer pursuant to this DPA. In doing so, CertKit acts as a "Data Processor" or "Service Provider" pursuant to Applicable Data Protection Law. Customer, in turn, is the "Controller" of Personal Data pursuant to the Applicable Data Protection Law for the purposes of this DPA.

2.2 Customer Authorization and Personal Data Processing

You appoint CertKit to process the Personal Data described in Annex I that is subject to the Agreement. Each party shall comply with its obligations under this DPA and Applicable Data Protection Law, including as related to the Processing of Personal Data. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired such Personal Data. Customer represents and warrants that it has all necessary rights, authorizations, and consents to transfer Personal Data to CertKit and for CertKit to process such Personal Data pursuant to the Agreement and this DPA. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or further Processing of Personal Data, or other disclosures of Personal Data, to the extent applicable under the CCPA or GDPR.

Customer shall be responsible for: (1) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and CertKit's Processing of Personal Data; and (2) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to CertKit and to permit the Processing of such Personal Data by CertKit for the purposes of performing its obligations under the Agreement, this DPA, or as may be required by Applicable Data Protection Laws. Customer shall notify CertKit of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Personal Data that would impact CertKit's ability to comply with the Agreement or applicable Data Protection Laws.

CertKit shall only process Personal Data on behalf of and in accordance with Customer's written instructions and shall treat Personal Data as confidential information. The parties agree that the Agreement (including this DPA), set out Customer's complete and final processing instructions to CertKit. Any processing outside the scope of these instructions shall require prior written agreement between the parties.

2.3 Service Provider

The parties acknowledge and agree that CertKit shall be a "service provider" to Customer for the purposes of the CCPA. To that end, CertKit is prohibited from the following: (a) selling or sharing Personal Data (except for such sharing that may be authorized pursuant to the Agreement or this DPA); (b) retaining, using, or disclosing personal data received from Customer for any purpose other than for the business purposes specified in the Agreement or this DPA, or as otherwise permitted by the CCPA; (c) retaining, using, or disclosing the personal data outside the direct business relationship between CertKit and Customer; and (d) combining Personal Data received from or on behalf of Customer with Personal Data it receives from or on behalf of other persons.

2.4 Prohibition of Sensitive Data

You will not submit, store, or send any sensitive data or special categories of personal data (collectively, "Sensitive Data") to us for processing, and you will not permit nor authorize any of your employees, agents, contractors, or data subjects to submit, store, or send any Sensitive

Data to us for processing. You acknowledge that we do not request or require Sensitive Data as part of providing the Service to you, that we do not wish to receive or store Sensitive Data, and that our obligations in this DPA will not apply with respect to Sensitive Data.

2.5 Confidentiality

CertKit shall take reasonable steps to ensure that its employees and contractors that process Personal Data from Customer are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality.

3. Data Deletion

3.1 Deletion During Term of Agreement

CertKit will enable you to delete Personal Data during the Term in a manner that is consistent with the functionality of the Service. If you use the Service to delete any Personal Data in a manner that would prevent you from recovering Personal Data at a future time, you agree that this will constitute an instruction to us to delete Personal Data from our systems in accordance with our standard processes and Applicable Data Protection Law. We will comply with this instruction as soon as reasonably practicable.

3.2 Deletion at Termination

When the Service Term expires, we will destroy any Customer Data (including Personal Data) in our possession or control. You acknowledge that you will be responsible for exporting, before the Term expires, any Personal Data you want to retain after the Term expires.

4. Data Security

4.1 Security Measures

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, CertKit will implement and maintain appropriate technical and organizational measures designed to protect Personal Data against Security Incidents and to preserve the security and confidentiality of Personal Data, as described in Annex II (collectively, the "Security Measures").

Customer acknowledges that Security Measures are subject to technical progress and development and that accordingly we may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service.

4.2 Security Incidents

Upon becoming aware of a Security Incident, we will notify you promptly and without undue delay, and will take reasonable steps to minimize harm and secure Personal Data. CertKit will provide Customer with information available to CertKit that Customer may reasonably require to comply with its obligations as Controller or Business, as may be applicable under the Applicable Data Protection Laws, to notify impacted Data Subjects or governmental authorities as may be required. Any notification that we send you pursuant to this Section will be sent to your Notification Email Address. We will not assess the contents of any Personal Data in order to identify information that may be subject to specific legal requirements. You are solely responsible for complying with any incident notification laws that may apply to you, and to fulfilling any third-party notification obligations related to any Security Incident(s). Our notification of or response to a Security Incident under this Section will not constitute an acknowledgement of fault or liability with respect to the Security Incident.

4.3 Customer Security Responsibilities

You agree that, without prejudice to our obligations under Sections 4.1 or 4.2: (i) you are solely responsible for your use of the Service, including making appropriate use of the Service to ensure a level of security appropriate to the risk in relation to Customer Data (including Personal Data), securing any account authentication credentials, systems, and devices you use to use the Service, and backing up your Customer Data. You understand and agree that we have no obligation to protect Customer Data that you elect to store or transfer outside of our or our Sub-processors' systems. You are solely responsible for evaluating whether the Service and our commitments under this Section 4 meet your needs, including with respect to your compliance with any of your security obligations under Applicable Data Protection Law.

4.4 Audit Rights

CertKit will maintain commercially reasonable internal security controls and auditing procedures to audit its Security Measures. Upon request, we will provide (on a confidential basis) a summary of our previous audit results.

While it is the parties' intention to rely on the provision of the above audit report(s) to verify our compliance with this DPA, we will allow an independent auditor (that is not a competitor of CertKit) that you select to conduct audits to verify our compliance with our obligations in this DPA. We will provide reasonable cooperation to Customer or its auditor in connection with such audits and will provide Customer or its auditor, upon request, all information reasonably necessary to demonstrate compliance with the DPA. CertKit and Customer will agree in advance on reasonable timing, scope, and security controls applicable to the Audit (including restricting access to CertKit trade secrets and data belonging to our other customers). Customer is responsible for any and all costs associated with the audit.

You agree not to exercise your audit rights under this section more than once in any rolling 12 month period, except (i) if required by a competent data protection authority under Applicable Data Protection Law; or (ii) after a Security Incident. If the Security Incident is caused by the Customer, we may charge you a reasonable fee for the audit that we will document in advance.

If you provide CertKit with notice of a security deficiency (detected through tests or audits performed under this section or otherwise), we will remediate the deficiency as appropriate, within a reasonable timeframe to be agreed upon by the parties.

4.5 Data Protection Officer

CertKit has appointed a Data Protection Officer where such appointment is required by Applicable Data Protection Law. The appointed person may be reached at hello@certkit.io.

4.6 Data Protection Impact Assessment and Prior Consultation

In the event that Customer considers that the Processing of Personal Data by CertKit requires a privacy impact assessment to be undertaken or requires assistance with any prior consultations to any supervisory authority of Customer pursuant to any Applicable Data Protection Laws, following written request from Customer, CertKit shall use reasonable commercial efforts to provide relevant information and assistance to Customer to fulfil such request, provided that CertKit may charge Customer on a time and materials basis in the event that CertKit considers, in its reasonable discretion, that such assistance is onerous, complex, frequent, or time consuming.

4.7 Business Continuity and Disaster Recovery

CertKit will maintain a business continuity and disaster recovery program designed to ensure the availability, integrity, and timely recovery of Customer Data in the event of a disruptive incident. The program will include, at a minimum: (i) regular backups of Customer Data to geographically separate locations; (ii) periodic testing of recovery procedures; and (iii) documented recovery time and recovery point objectives appropriate to the nature of the Service. CertKit will review and update its disaster recovery program periodically to reflect changes in infrastructure, risk, and industry practice.

5. Data Subject Rights

You acknowledge that the Service may enable you to: (i) access the Customer Data; (ii) rectify inaccurate Customer Data; (iii) restrict the processing of Customer Data; (iv) delete Customer Data; and (v) export Customer Data.

To the extent that you cannot access the relevant Personal Data within the Service, we will provide you, at your expense, with all reasonable and timely assistance to enable you to respond to: (i) requests from data subjects who wish to exercise any of their rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from a Data Subject, supervisory authority, or other third party in connection with the processing of the Customer Data.

If CertKit receives a request from a Data Subject under any Applicable Data Protection Laws in respect to Personal Data Processed on behalf of Customer, CertKit will promptly notify Customer of the request.

6. International Data Transfer

6.1 Data Storage

You agree that we may store and process Customer Data in Canada and other countries in which we or our Sub-processors maintain Data Processing operations. The parties will ensure that such transfers are made in compliance with Applicable Data Protection Law, including as set forth in Section 6.2.

6.2 Transfer of Data out of European Economic Area (EEA)

In the event that Customer transfers Personal Data from within the EEA to CertKit at a location outside the EEA, Customer (as data exporter) and CertKit (as data importer) shall enter into the Standard Contractual Clauses as set forth in Appendix 1 to this DPA (or as subsequently amended by the European Commission or data protection regulators in the EEA). Module 2 (Controller to Processor) will apply where Customer is a Controller of Personal Data and CertKit is a Processor of Personal Data. Module 3 (Processor to Processor) will apply where Customer is a Processor of Personal Data and CertKit is a Processor of Personal Data. In the event that the Standard Contractual Clauses cease to be recognized as an appropriate mechanism for the transfer of Personal Data to an entity located outside the EEA, Customer shall cooperate with CertKit to identify and implement an alternative mechanism to the extent required by the Applicable Data Protection Laws.

6.3 Standard Contractual Clauses

The parties agree that (i) for the purposes of the descriptions in the Standard Contractual Clauses, CertKit is the "Data Importer" and you are the "Data Exporter" (notwithstanding that you may be located outside Europe and/or you may be acting as a processor on behalf of third party controllers); and (ii) 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. In particular, nothing in the DPA shall exclude the rights of third-party beneficiaries granted under the Standard Contractual Clauses.

7. Sub-processors

7.1 Consent to Engagement

You specifically authorize us to engage third parties as Sub-processors. CertKit may engage such Sub-processors as it considers reasonably appropriate for the Processing of Personal Data received from Customer in accordance with the Agreement and this DPA. Whenever we engage a Sub-processor, we will enter into a written contract with that Sub-processor which imposes data protection terms that require the Sub-processor to protect Personal Data to an

equivalent standard required under this DPA, and we shall remain responsible for the Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause us to breach any of our obligations under this DPA.

7.2 Objections and Sole Remedy

CertKit shall notify Customer of the addition or replacement of any Sub-processor to the list in Annex III. Within ten (10) days of such notice, Customer may object to the appointment of any such Sub-processor on reasonable grounds that must be provided to CertKit in writing (each, an "Objection"). The parties agree to work together in good faith to address Customer's reasonable Objection. If the parties are unable to reasonably resolve the Objection within 30 days of CertKit receiving the objection, you may, as your sole remedy and our sole liability for your Objection, terminate the Agreement for your convenience, and without further liability to either party. We will not owe you a refund of any fees you have paid in the event you decide to terminate the Agreement pursuant to this Section.

8. Miscellaneous

8.1 Precedence

There are no third-party beneficiaries to this DPA. Except as expressly provided herein, nothing in this DPA will be deemed to waive or modify any of the provisions of the Agreement, which otherwise remains in full force and effect. Specifically, nothing in this DPA will affect any of the terms of the Agreement relating to CertKit's limitations of liability, which will remain in full force and effect. If you have entered into more than one Agreement with us, this DPA will amend each of the Agreements separately. In the event of a conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA will control.

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

8.2 Governing Law

This Agreement shall be governed by, and construed in accordance with, the law of the State of Minnesota USA and the courts located in Washington County, Minnesota shall have exclusive jurisdiction to hear any dispute or other issue arising out of, or in connection with, this Agreement, except where otherwise required by Applicable Data Protection Law.

8.3 Insurance

CertKit will maintain commercially reasonable cyber liability insurance coverage appropriate to the nature and scope of the Service. Upon written request, CertKit will provide Customer with a certificate of insurance evidencing such coverage.

9. Changes in Applicable Data Protection Laws

Notwithstanding anything to the contrary in the Agreement (including this DPA), in the event of a change in Applicable Data Protection Laws or a determination or order by a supervisory authority or competent court affecting this DPA or the lawfulness of any processing activities under this DPA, we reserve the right to make any amendments to this DPA as are reasonably necessary to ensure continued compliance with Applicable Data Protection Law or compliance with any such orders.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the date signed.

Customer: . . . . . .

Signature:. . . . . .
Name: . . . . . .
Title: . . . . . .
Date Signed: . . . . . .

TrackJS LLC

Signature: 
Name: Todd Gardner
Title: CEO
Date Signed: April 21, 2026

Appendix 1

Standard Contractual Clauses

SECTION I

Clause 1 - Purpose and scope

1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) 1] for the transfer of data to a third country.
2. The Parties:

1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I (hereinafter each 'data exporter'), and
    1. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

2. These Clauses apply with respect to the transfer of personal data as specified in Annex I.
3. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    2. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    3. Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c), and (d) and Clause 8.9(a), (c), (d), (e), (f), and (g);
    4. Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d), and (e);
    5. Clause 12(a), (d) and (f);
    6. Clause 13;
    7. Clause 15.1(c), (d) and (e);
    8. Clause 16(e);
    9. Clause 18(a) and (b).
2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer Controller to Processor

8.1 Instructions

3. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
4. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

4. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
5. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
6. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
7. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for

the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.

8.8 Onward transfers

3. The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union 2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
3. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
    10. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
    11. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
    12. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

4. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
5. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
6. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
7. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
8. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer Processor to Processor

8.1 Instructions

5. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
6. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
7. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
8. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall

continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

8. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
9. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
10. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

11. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

4. The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
    13. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
    14. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
    15. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
    16. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

4. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
5. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

6. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
7. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
8. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
9. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
10. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

MODULE TWO: Transfer Controller to Processor

9. OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
10. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. 3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
11. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
12. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data

importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

13. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer Processor to Processor

9. OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub processors at least thirty (30) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
10. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
11. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
12. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
13. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

MODULE TWO: Transfer Controller to Processor

12. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
13. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
14. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer Processor to Processor

5. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
6. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
7. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11 - Redress

11. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
12. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
13. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
14. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

17. refer the dispute to the competent courts within the meaning of Clause 18.

15. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
16. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
17. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

14. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
15. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
16. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
17. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
18. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
19. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
20. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

15. The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I, shall act as competent supervisory authority.

16. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

8. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
9. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
14. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
    18. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards 5];
    19. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
15. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
16. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

MODULE TWO: Transfer Controller to Processor

17. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
18. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

MODULE THREE: Transfer Processor to Processor

19. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.
20. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

18. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
21. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    20. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
22. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
23. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
24. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
25. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

17. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to

do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

18. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
19. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

10. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
11. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
12. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
21. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    21. the data importer is in substantial or persistent breach of these Clauses; or
    22. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

22. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
23. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU)

2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of The Republic of Ireland.

Clause 18 - Choice of forum and jurisdiction

19. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
20. The Parties agree that those shall be the courts of The Republic of Ireland.
21. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
22. The Parties agree to submit themselves to the jurisdiction of such courts.

IN WITNESS WHEREOF, this Standard Contractual Clauses is entered into and becomes a binding part of the Agreement with effect from the date signed.

Customer: . . . . . .

Signature:. . . . . .
Name: . . . . . .
Title: . . . . . .
Date Signed: . . . . . .

TrackJS LLC

Signature: 
Name: Todd Gardner
Title: CEO
Date Signed: April 21, 2026

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

ANNEX I

Data Processing Description

A. List of Parties

Data exporter(s):

Name: You, the Customer (as defined in the DPA).

. . . . . .

Address: Customer's address.

. . . . . .

. . . . . .

Contact person's name, position, and contact details:

. . . . . .

. . . . . .

Role: (controller/processor)

. . . . . .

Signature and date

. . . . . .

. . . . . .

Data importer(s):

Name:

TrackJS LLC, a Minnesota Limited Liability Company

Address:

2112 Broadway St NE STE 225 PMB 25, Minneapolis, MN 55413-3081 USA

Contact person's name, position, and contact details:

Data Protection Officer, hello@certkit.io

Role:

processor

Signature and date

April 21, 2026

B. Data Processing Description

Subject Matter: CertKit's automated TLS certificate management services to Customer and related technical support.

Categories of data subjects: Personal data transferred concern the following data subjects:

26. Customer's employees, contractors, or authorized users who access the Service
27. Customer's technical contacts associated with certificate management operations

Categories of personal data:

Data exporter may submit Personal Data to the Service (as this term is defined in the Terms of Service), the extent of which is controlled and determined by the data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Personal Data:

20. account information (email address, display name, hashed password);
21. domain names and hostnames configured in the Service;
22. certificate lifecycle data (issuance, renewal, expiration, deployment status);
23. Agent and deployment configuration data (host identifiers, server types, deployment paths);
24. operational and audit logs (service actions, timestamps, diagnostic data);
25. billing and payment metadata (processed by third-party payment provider)

Sensitive data:

Any Personal Data transferred to the data importer is determined and controlled by the data exporter. As such, the data exporter controls the content of Personal Data and is solely responsible for ensuring the legality of the data transferred to the data importer. The Data Processing Agreement expressly prohibits the transfer of special categories of data to the data importer.

Frequency of the transfer: continuous

Nature of the processing:

Automated TLS certificate lifecycle management services as described in this Agreement, including certificate issuance, renewal, deployment, verification, and monitoring.

Purpose(s) of the data transfer and further processing:

CertKit will process personal data submitted to, stored on, or sent via the Service for the purpose of providing the Service and related technical support in accordance with this DPA.

The period for which the personal data will be retained:

Throughout the Term of the Agreement plus the period from expiry of the Term until deletion of Personal Data by CertKit in accordance with the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

13. OVH Limited
    23. *Subject matter:* Hosting
    24. *Nature of Processing:* Infrastructure hosting services pursuant to the data importer's agreement with this entity.
    25. *Duration of the processing:* The duration of the data importer's agreement with this entity.
14. Stripe, Inc.
    26. *Subject matter:* Payment processing
    27. *Nature of Processing:* Payment and billing services pursuant to the data importer's agreement with this entity.
    28. *Duration of the processing:* The duration of the data importer's agreement with this entity.
15. Mailgun Technologies, Inc.
    29. *Subject matter:* Email notifications
    30. *Nature of Processing:* Transactional email services pursuant to the data importer's agreement with this entity.
    31. *Duration of the processing:* The duration of the data importer's agreement with this entity.
16. Amazon Web Services, Inc.
    32. *Subject matter:* Offsite data backup
    33. *Nature of Processing:* Cloud storage services pursuant to the data importer's agreement with this entity.
    34. *Duration of the processing:* The duration of the data importer's agreement with this entity.
17. PostHog, Inc.
    35. *Subject matter:* Product analytics
    36. *Nature of Processing:* Product usage analytics services pursuant to the data importer's agreement with this entity.
    37. *Duration of the processing:* The duration of the data importer's agreement with this entity.
18. Google LLC (Google Workspace)
    38. *Subject matter:* Business email and productivity
    39. *Nature of Processing:* Email communications and document storage services pursuant to the data importer's agreement with this entity.
    40. *Duration of the processing:* The duration of the data importer's agreement with this entity.

19. HubSpot, Inc.
    41. *Subject matter:* CRM and support
    42. *Nature of Processing:* Customer relationship management and support request tracking services pursuant to the data importer's agreement with this entity.
    43. *Duration of the processing:* The duration of the data importer's agreement with this entity.

C. Competent Supervisory Authority

The Irish Data Protection Commissioner.

ANNEX II

Technical and Organizational Security Measures

This Annex II forms part of the Agreement and describes the security measures implemented by the Data Importer in accordance with Clauses 8.6 and 10(b).

Data Importer will maintain administrative, physical, and technical safeguards for protection of security, confidentiality, and integrity of data processed on behalf of the Data Exporter.

Physical Security

Controls are in place to prevent unauthorized physical access to facilities holding Data Exporter's data. Controls must include:

- Access control system
- Issuing of electronic or physical keys to personnel
- Door locks
- Alarms and video surveillance
- Logging of facilities entrance and exit

Application Security

Controls are in place to prevent unauthorized access to IT systems that store or process Data Exporter's data. Controls must include:

- Management of system access
- Network isolation and segmentation of systems (firewalls and networks)
- System patching and maintenance
- Password policy
- Access to systems governed by Data Ownership processes

Data Security

Controls are in place to prevent unauthorized access or loss of Data Exporter's data. Controls must include:

- Data Classification policy
- Role-based access rights
- Access rights reviewed and approved by Data Owners
- Data is encrypted in transit
- Data is backed up regularly to offsite locations

Cryptographic Key Material Security

Additional controls are in place specific to the protection of TLS private keys and related cryptographic material managed through the Service:

- Access to key storage is limited to essential service operations
- Access to key material is logged and monitored
- Key material is encrypted at rest
- Key material is transmitted only over encrypted channels

Logging, Monitoring, and Auditing

Controls are in place to ensure that system and data access is logged and an audit trail is maintained. Controls must include:

- Logging and alerting access to IT systems
- Logging user activity on IT systems
- Logs are audited regularly for irregularities

Sub-Processor Technical and Organizational Security Measures

Controls to be taken by the sub-processor to be able to provide assistance to the controller and data exporter include the following:

- encryption of Personal Data in transit;
- measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- 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;
- processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing;
- measures for user identification and authorization;
- measures for the protection of data during transmission;
- measures for the protection of data during storage;
- measures for ensuring physical security of locations at which Personal Data are processed;
- measures for ensuring events logging;
- measures for ensuring system configuration, including default configuration;
- measures for internal IT and IT security governance and management;
- measures for certification/assurance of processes and products;
- measures for ensuring data minimisation;
- measures for ensuring data quality;
- measures for ensuring limited data retention;
- measures for ensuring accountability; and
- measures for allowing data portability and ensuring erasure

Measures and Assurances Regarding Government Surveillance

- As of the date of this DPA, CertKit has not received any customer data requests from governments (wiretap orders, pen register/trap and trace orders, search warrants, orders issued under 18 U.S.C. § 2703(d), subpoenas, or emergency requests for disclosure).
- No court has found CertKit to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.
- CertKit shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).
- CertKit shall use all available legal mechanisms to challenge any demands for data access through national security process that CertKit receives, as well as any non-disclosure provisions attached thereto.
- CertKit shall take no action pursuant to U.S. Executive Order 12333.
- CertKit will notify Customer if CertKit can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

ANNEX III

List of Sub-processors

CertKit conducts reasonable due diligence and security assessments of sub-processors it engages for the storing and/or processing of Personal Data, and enters into agreements with sub-processors that contain provisions similar or more stringent than those provided for in this DPA. Data importer will work directly with sub-processors, as necessary, to provide assistance to Customer.

The following Sub-processors of Customer Data have been reviewed and approved by CertKit.

OVH Limited
1801 McGill College Ave.
Suite 800
Montreal, Quebec H3A 2N4
Canada
Cloud infrastructure hosting services.

Stripe, Inc.
354 Oyster Point Blvd
South San Francisco, CA 94080
United States of America
Payment processing and billing services.

Mailgun Technologies, Inc.
112 E Pecan St. #1135
San Antonio, TX 78205
United States of America
Transactional email services.

Amazon Web Services, Inc.
410 Terry Avenue North
Seattle, WA 98109
United States of America
Offsite data backup and cloud storage services.

PostHog, Inc.
2261 Market Street #4008
San Francisco, CA 94114
United States of America
Product usage analytics services.

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States of America
Business email (Google Workspace) and productivity services.

HubSpot, Inc.
25 First Street, 2nd Floor
Cambridge, MA 02141
United States of America
Customer relationship management and support request tracking.

ANNEX IV

Business Related Terms

This Annex IV forms part of the Agreement and describes additional business-related terms as permitted by Clause 2 of the Standard Contractual Clauses, provided that they do not contradict with the Clauses. Accordingly, this Annex specifies the parties' obligations under the specific clauses identified below.

Clause 8.9: Audit

- Data Exporter acknowledges and agrees that it exercises its audit right under Clause 8.9 by instructing data importer to comply with the audit measures described in Section 4.4 of the Data Processing Agreement.

Clause 12 - Liability

- Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Data Processing Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.