

Hunter®

 **Hydrawise™ Ready**
IRRIGATION CONTROLLERS

Hydrawise Software/App Owner's Manual



Table of Contents

Table of Contents	2
Hydrawise API Information	3
Hydrawise API Terms of Use	4
Data Processing Addendum	11

Hydrawise API Information

Hydrawise has two available APIs:

- **RESTful API**
- **Graph QL & oAuth 2.0 API**

The API requires a key that can be obtained from your Hydrawise account using the steps below:

1. Click on the **My Account** icon  (for mobile devices, click the hamburger icon )
2. Click **Account Details**.
3. In the **Account Settings** box, choose **Generate API Key**.

RESTful API

The RESTful API is ideal for homeowners and noncommercial Hydrawise users.

It allows you to monitor multiple controllers in a single Hydrawise account.

It provides the following information:

- Controller names
- Zone number and name
- Time until next run
- Currently running
- Length of run time
- Manual start and stop
- Manual run all stations
- Suspend a zone or all zones

In order to ensure scalability and stability we have the following API limits

- The limit is 3 calls to start/stop/suspend a zone per 30 seconds.
- There is an additional limit across the entire API of 30 calls in a 5 minute period per user.

The API documentation is at the bottom of support page.

Graph QL & oAuth 2.0 API

The Graph QL & oAuth 2.0 API is ideal for commercial applications, home automation, and government agencies.

It is rate limited and provides a secure GDPR & CCPA compliant API.

It provides the following information:

- Controller names
- Zone number and name
- Time until next run
- Currently running
- Length of run time
- Sensor status
- Manual start and stop
- Manual run all stations
- Suspend a zone or all zones
- Unsuspend a zone or all zones

If you have additional questions regarding the API please email anthony.long@hunterindustries.com.

To use any Hydrawise API, you agree to accept our [API Terms of Use](#) ^[1], [Data Processing Addendum](#) ^[2], [Terms and Conditions](#) ^[3] and [Privacy Statement](#) ^[4].

Stay up to date with Hydrawise



Latest Features

^[5]

Hydrawise API Terms of Use

These Terms of Use (Agreement) are an agreement between Hunter Industries (“Hunter”) and You governing the use of Hydrawise Application Programming Interfaces (the “APIs”).

PLEASE READ THESE TERMS OF USE CAREFULLY BEFORE USING THE APIS. BY ACCESSING AND USING OR CONTINUING TO USE THE APIS, YOU IRREVOCABLY AGREE TO ABIDE BY THE FOLLOWING TERMS AND CONDITIONS.

1. Terms

Hunter Industries is a family-owned global company that provides high quality, efficient solutions for the irrigation, outdoor lighting, and custom molding industries. Our diverse array of products can be seen everywhere from residential landscapes to stadiums, national landmarks, theme parks, city parks, commercial complexes, hotels, and municipal buildings around the world.

Hydrawise is a product and service provided by Hunter Industries. All rights, obligations, and ownership of Hydrawise reside with Hunter Industries.

2. License

Hunter Industries grants you (the licensee) a limited, non-exclusive, revocable, non-sublicensable, non-transferable license to use the APIs in order to develop and distribute applications that interoperate with Hunter products and services.

Both commercial and non-commercial uses of the APIs are acceptable. Any commercial use of the APIs must be submitted for prior and written authorization of Hunter Industries.

3. Restriction

Except as expressly and unambiguously authorized under this Agreement, the license granted is subject to the following restrictions:

3.1. You may not use the Hunter Hydrawise APIs in a product or service that competes with products or services offered by Hunter Industries, except prior and written authorization given by Hunter Industries. For that purpose, please contact support@hydrawise.com.

3.2. When using the Hunter Hydrawise API, before accessing a user's personal data, you must ensure that you have the express permission of this user to access his data and you fulfil all applicable law and regulation. You will not attempt to access data for which you have not obtained adequate permission.

3.3. You may not use the Hunter Hydrawise API in any manner or for any purpose that violates any law or regulation, any right of any person, including but not limited to intellectual property rights, rights of privacy, or rights of personality, personal data protection, or in any manner inconsistent with the Terms of Use. You shall not misappropriate, reproduce, modify, distribute, decompile, disassemble, or reverse engineer any part of the Hunter Hydrawise APIs, the Hunter Industries products, or any data provided by Hunter industries.

3.4. Those APIs are currently provided free of charge, but Hunter Industries reserves the right to charge for those APIs in the future.

3.5. All calls to the Hunter Hydrowise APIs must reference the Hunter Hydrowise APIs Key issued to you as an approved licensee. You must keep this APIs Key confidential and may not share it with any third party.

3.6. You may not sell, lease, share, transfer, or sublicense your Hunter Hydrowise APIs key or Hunter Hydrowise APIs access thereto without Hunter Industries prior, express, written permission.

3.7. In order to ensure a consistent access for all client applications, Hunter Industries reserves the right to limit the Hunter Hydrowise APIs calls frequencies and will inform you of such limitations. In the case where your use of the APIs exceeds those limits, you should contact Hunter Industries.

3.8. Hunter Industries reserves the right, without notice and at its sole discretion, to change any application's name or description (e.g. if considered inappropriate or infringing any third party intellectual property rights)

3.9. Hunter Industries reserves the right, without notice and at its sole discretion, to change, remove, delete or use any application's icon (e.g. if considered inappropriate or infringing any third party intellectual property rights)

4. Personal Data

The API contains data that can be deemed personal data, in itself, or when cross-matched with other data, namely:

4.1. User Information

- Customer Name
- Street Address
- City
- Country
- Time Zone
- Email Address
- Language

4.2. Irrigation and Weather

- Controllers, Devices including Sensors (Rain, Wind, Soil Moisture and Others) refer to the product specifications.
- Home landscape information (Controller, sensors, and zone names)
- Irrigation schedules details
- Device information such as Wi-Fi status, radio status, battery level, location, station, and modules names

4.3. Security Events (Irrigation activation, alert detected, user program changes, etc.)

This data is processed by Hunter Industries as per its standard Hydrowise Terms and Conditions and its Privacy Policy.

5. Processing of Data – Additional

You understand that, by processing the API personal data according to means and purposes you autonomously decide, you become a data controller of this processing. You shall, therefore, be aware of, and comply with your obligations as such and make sure that the processing you are the controller of is lawful (e.g. respect the purpose limitation and data minimization principles, keep data only as long as necessary, take care of administrative formalities, etc.).

You shall, amongst other obligations:

5.1. Give appropriate information to users about the processing you are the controller of before you start carrying it on.

5.2. Obtain, when necessary, prior consent from users, before accessing a user's personal data. This consent shall be clearly given, free, specific, and informed.

5.3. Enable your application's users to exercise their rights of access, rectification, restriction, erasure and their right to object to data processing, notably by giving them a point of contact towards whom they can exercise these rights.

5.4. Take the necessary organizational and technical measures to ensure the protection of the data.

5.5. Ensure a high degree of security regarding the API.

5.5.1. If you are a legal entity, you shall make sure that only the persons who need to access the API are able to do so and that the API's Key issued to you by Hunter Hydrowise is known only by these persons.

5.5.2. You shall ensure that the security, availability, authenticity, integrity and confidentiality of the personal data contained in the API are not compromised by your fault or your negligence. You shall warn Hunter Industries immediately if you become aware of a breach in the security, availability, authenticity, integrity or confidentiality of the personal data contained in the API.

5.5.3. You shall always access the API with a secure Internet connection.

5.6. You understand that any breach in the obligations will result, at least, in the withdrawal of your access to the API, and that Hunter Industries will be able to seek your liability.

5.7. This Agreement incorporates the Hunter Data Processing Addendum ("Addendum")

(<https://support.hydrawise.com/hc/en-us/articles/13660306549147> ^[2]) when you use the APIs to process Customer Data (as defined in the Addendum). The Addendum incorporates the Standard Contractual Clauses (“SCCs”) between controllers and processors. The SCCs will only apply when: (i) the GDPR applies to your use of the APIs to process Customer Data; and (ii) Customer Data is transferred either directly or via onward transfer, to a country outside of the European Economic Area not recognized by the European Commission as providing an adequate level of protection for personal data subject to GDPR (together a “Data Transfer”).

6. Property

6.1. The Hunter Hydrawise APIs and Hunter Hydrawise Brand are the property of Hunter Industries, and subject to the intellectual property rights of Hunter Industries. You may use the brand « Hunter Hydrawise » in the name of your application and its content, only to indicate the source of the data, the affiliation between your application and our services or the compatibility of your application with a Hunter Hydrawise account. You may not use « Hunter Hydrawise » or any variation thereof in a deceptive manner, that would mislead the user to believe that your application would be an official production of Hunter Industries.

6.2. Any use of the brand « Hunter Hydrawise » shall be validated in writing by Hunter Hydrawise before any distribution of your products and/or services.

6.3. Hunter Industries is and remains the sole owner of all technical and/or scientific information and knowledge and in particular know-how, inventions, manufacturing secrets, commercial secrets, data, databases, software (in source- codes and object-codes versions), files, plans, diagrams, designs, formulae and/or any other types of information, in any form whatsoever, patentable or not and/or patented or not, and all intellectual property rights relating thereto (collectively, the “IPR”), in relation with Hunter Industries products.

6.4. The Content provided through those APIs remains property of Hunter Industries. This agreement in no way conveys any ownership rights to you in any Hunter Hydrawise data and content accessed through those APIs.

7. Modification and Termination

7.1. Hunter Industries may update or modify the Hunter Hydrawise APIs or APIs Terms of Use from time to time at its sole discretion. You are responsible for monitoring these changes and complying with the most recent Hunter Hydrawise APIs Terms of Use. If any change is unacceptable to you, your only recourse is to terminate this agreement by notifying it in writing to Hunter Industries and ceasing all use of the Hunter Hydrawise APIs. Your lack of answer and/or continued access or use of the Hunter Hydrawise APIs will constitute binding acceptance of the change.

7.2. You may terminate any license granted to you hereunder at any time by notifying it to Hunter Industries and ceasing your access to and use of the APIs and any use of the Hunter Hydrawise Data.

7.3. Hunter Industries may change, suspend or discontinue the Hunter Hydrawise APIs at any time for any reason, without notice.

7.4. Hunter Industries reserves the right, in its sole discretion, to terminate your license to use the Hunter Hydrawise APIs, and to block or prevent future access to and use of the Hunter Hydrawise APIs, by notification sent by any written means (letter; telecopy; email...), with a notice period of one (1) month.

7.5. Upon any termination of these Hunter Hydrawise APIs Terms of Use, you shall promptly delete and remove all calls to the Hunter Hydrawise APIs from all web pages, scripts, widgets, applications, other software or hardware in your possession or under your control, and any support whatsoever.

8. NO WARRANTIES

THE HUNTER HYDRAWISE APIS, DATA AND SERVICES ARE PROVIDED ON AN 'AS IS' AND 'AS AVAILABLE' BASIS WITHOUT ANY WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. THE HUNTER INDUSTRIES PARTIES DISCLAIM ALL WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF OPERATION, MERCHANTABILITY, NON-INFRINGEMENT OF THIRD PARTIES RIGHTS, ACCURACY, RELIABILITY, TIMELINESS, AND FITNESS FOR PARTICULAR PURPOSE. YOU EXPRESSLY AGREE THAT USE OF THIS API AND SERVICES, INCLUDING ALL CONTENT OR DATA DISTRIBUTED BY, DOWNLOADED OR ACCESSED FROM OR THROUGH THIS SERVICE, IS AT YOUR SOLE RISK.

9. LIMITATION OF LIABILITY

IN NO EVENT SHALL ANY HUNTER HYDRAWISE PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST DATA OR BUSINESS INTERRUPTION) ARISING OUT OF THE USE OR INABILITY TO USE, OR RESULTING FROM USE OF THE HUNTER HYDRAWISE APIS AND ITS CONTENT, WHETHER SUCH DAMAGES ARE BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL THEORY, EVEN IF ANY HUNTER HYDRAWISE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

10. Indemnification

You hereby agree to indemnify, defend and hold Hunter Industries, and its subsidiaries, affiliates, officers, directors, agents, licensors and licensees (collectively, the "Indemnified Parties") harmless from and against any and all liability and costs incurred by the Indemnified Parties in connection with any claim, loss, damage (actual and consequential), suit or judgement arising out of your or your users' use of the Hunter Hydrawise APIs, including, without limitation, litigation costs and attorneys' fees, of every kind and nature. In such a case, Hunter Industries will provide you with written notice of such claim, suit, or

action. Hunter Industries reserves the right, at its own expense, to assume the exclusive defense and control of any matter subject to indemnification by you.

11. Miscellaneous

11.1. This Agreement is governed by California law and the laws of the United States of America. Any dispute resulting from out of the interpretation, performance or consequences of this Agreement shall be settled by negotiation in good faith by the Parties.

11.2. If the Parties have not reached an agreement within one (1) month after notification of the dispute by one Party to the other Party by registered mail with recorded delivery, this dispute shall be referred to the exclusive jurisdiction of the Courts within the realm of the California, United States of America.

11.3. If any provision of these API Terms of Use is found to be invalid by any court having competent jurisdiction, the invalidity of such provision shall not affect the validity of the remaining provisions of these APIs Terms of Use, which shall remain in full force and effect.

11.4. Failure of Hunter Industries to act on or enforce any provision of these APIs Terms of Use shall not be construed as a waiver of that provision or any other provision in these APIs Terms of Use.

11.5. No waiver shall be effective against Hunter Industries unless made by an authorized officer of Hunter Industries in writing, and no such waiver shall be construed as a waiver in any other or subsequent instance.

11.6. Except as expressly agreed by Hunter Industries and you, these APIs Terms of Use constitutes the entire Terms of Use between you and Hunter Industries with respect to the subject matter, and supersedes all previous or contemporaneous agreements, whether written or oral, between the you and Hunter Industries with respect to the subject matter.

11.7. The section headings are provided merely for convenience and shall not be given any legal import.

11.8. The terms of this Agreement will inure to the benefit of our successors, assigns, licensees, and sublicensees.

11.9. Any information submitted or provided by you to the Services might be publicly accessible. Important and private information should be protected by you. Hunter Industries is not liable for protection of privacy of electronic mail or other information transferred through the Internet or any other network that you may use. The collection and processing of Personal Data, made when you use the Services, is carried out in accordance with the Hunter Industries Privacy Policy (<https://www.hunterindustries.com/privacy-policy>)

Data Processing Addendum

This Data Processing Addendum ("Addendum") supplements the Hunter Hydrawise Terms of Use Agreement, as updated from time to time between You and Hunter Industries, governing Your use of the APIs (the "Principal Agreement"). This Addendum is an agreement between You ("Vendor") acting on its own behalf and as agent for each Vendor Affiliate; and (ii) Hunter Industries ("Company") acting on its own behalf and as agent for each Company Affiliate.

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

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "Applicable Laws" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; b) UK laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to UK Data Protection Laws; (c) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "Company Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "Company Group Member" means Company or any Company Affiliate;

1.1.4 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.5 "Contracted Processor" means Vendor or a Subprocessor;

1.1.6 "Data Protection Laws" means EU Data Protection Laws, UK Data Protection Laws

and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "EEA" means the European Economic Area.

1.1.8 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR; "UK Data Protection Laws" means the Data Protection Act 2018 and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

1.1.9 "GDPR" means EU General Data Protection Regulation 2016/679 and the UK GDPR;

1.1.10 "Restricted Transfer" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section [6.4.3 or] 12 below;

1.1.11 "Services" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.12 "Standard Contractual Clauses" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.13 "Subprocessor" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.14 "Vendor Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. Processing of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 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, Vendor and each Vendor Affiliate shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a

Personal Data Breach.

6. Subprocessing

6.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment: Neither Vendor nor any Vendor Affiliate shall appoint (or disclose any Company Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Company Group Member and Company has been provided with a reasonable written explanation of the steps taken.

6.4 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group

Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.4.4 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of

Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Vendor shall:

7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal Data

10.1 Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within 30 days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

10.2 Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within 30 days of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any

Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within 30 days of the Cessation Date.

10.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within 30 days of the Cessation Date.

11. Audit rights

11.1 Subject to sections [11.2 to 11.4], Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 [A Company Group Member may only mandate an auditor for the purposes of section 11.1 if the auditor is identified in the list set out in Annex 3 to this Addendum, as that list is amended by agreement between the parties in writing from time to time. Vendor shall not unreasonably withhold or delay agreement to the addition of a new auditor to that list.]

11.4 [Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on

those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.4.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.4.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

11.4.3 for the purposes of more than [one] audit or inspection, in respect of each Contracted

Processor, in any [calendar year], except for any additional audits or inspections which:

11.4.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably

considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or

11.4.3.2 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.]

12. Restricted Transfers

12.1 Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 [Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a Vendor Affiliate, Vendor's or the relevant Vendor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Subprocessor.]

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner

which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Company may:

13.4.1 by at least [30 (thirty) calendar days] written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Company gives notice under section 13.4.1:

13.5.1 [Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and]

13.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 [and/or 13.5.1].

13.6 If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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.

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data are set out in the Principal Agreement and this Addendum.

The types of Company Personal Data to be Processed are set out in the Principal Agreement and this Addendum.

The categories of Data Subject to whom the Company Personal Data relates are set out in the Principal Agreement and this Addendum.

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

This attachment is attached to and forms part of the Data Processing Addendum or other agreement between You and Hunter Industries governing the processing of Company Personal Data (the “Addendum”).

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

Hunter Industries (the “data exporter”) and You (the “data importer”), each separately a “party” and together “the parties”,

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

Background

The data exporter has entered into a data processing addendum (“ADDENDUM”) with the data importer. Pursuant to the terms of the ADDENDUM, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the

protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.]

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or

have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance

with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

to the data exporter.

Clause 6

Liability

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

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

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

Clause 7

Mediation and jurisdiction

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

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

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

APPENDIX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as “Company” in the Addendum.

Address: The address for Company as otherwise specified in the Addendum or the Principal Agreement.

Contact person’s name, position and contact details: The contact details associated with Company as specified in the Addendum or the Principal Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in the Addendum or Principal Agreement.

Signature and date: By using the API to transfer Company Personal Data to Third Countries, the data exporter will be deemed to have signed this Appendix I.

Role (controller/processor): Controller

Data importer(s):

Name: “You” or “Vendor” as identified in the Addendum.

Address: The address You specified in the Addendum or the Principal Agreement.

Contact person’s name, position and contact details: The contact details You specified in the Addendum or the Principal Agreement or as provided otherwise in writing to Company.

Activities relevant to the data transferred under these Clauses: The activities specified in the Addendum or the Principal Agreement.

Signature and date: By transferring Company Personal Data to Third Countries, the data importer will be deemed to have signed this Annex I.

Role (controller / processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Categories of data subjects include Customers or as otherwise specified in the Addendum or the Principal Agreement.

Categories of personal data transferred:

Categories of personal data include e-mail addresses, names, and geo-location or as otherwise specified in the Addendum or the Principal Agreement.

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

The data exporter will not include sensitive personal data.

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

Personal data is transferred in accordance with Company's instructions as described in the Addendum or the Principal Agreement.

Nature of the processing:

The nature of the processing is described in the Addendum or the Principal Agreement.

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

To provide the services associated with the API.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Not applicable because the data exporter determines the duration of processing in accordance with the terms of the Addendum or the Principal Agreement.

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

The subject matter, nature and duration of the processing are described in the Addendum or the Principal Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

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

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

APPENDIX II:

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

Description of the technical and organisational measures implemented by the 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:

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in the Addendum or the Principal Agreement.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

The technical and organisational measures that the data importer will impose on sub-processors are described in the Addendum or the Principal Agreement.