IPI Data Protection Addendum

Last updated: 03 February 2023

DOCUMENT INFORMATION

DOCUMENT TITLE:	IPI Data Protection Addendum
SECURITY CLASSIFICATION:	Confidential
AUTHOR:	Amy Chesson
DATE:	03/02/2023

DISCLAIMER

This document contains confidential information about IP Integration Ltd. No part of its contents may be used, copied, disclosed, or conveyed to any other party in any manner without the prior written permission of IP Integration Ltd.

This document is stored and maintained electronically. If any doubt exists as to the current version of the printed copy, reference should be made to the Document Owner/Manager for verification. Proposed changes must also be sent to the Document Owner.

All intellectual property contained within this document remains solely the property of IP Integration Ltd and cannot be copied, disclosed, or conveyed to any other party in any manner without the prior written permission of IP Integration Ltd.

This data protection addendum (the '**IPI Data Protection Addendum**') forms part of the Agreement between the Supplier and the Customer (as defined below).

1. Interpretation

1.1 The following definitions and rules of interpretation apply in this IPI Data Protection Addendum:

Agreement: the agreement between the Supplier and the Customer, which incorporates this IPI Data Protection Addendum by reference.

Applicable Laws: all applicable laws, statutes, regulation from time to time in force.

Customer: the company identified as the 'Customer' in the Agreement.

Business Contact Information: personal data provided or made available by one party to the other which is operationally required for the performance of the Agreement (business contact information such as names, email addresses and telephone numbers) relating to that party's employees or representatives. For the avoidance of doubt, 'party' in this context means either the Supplier and/or the Customer.

Communications Data: any Personal Data required to be processed by the Supplier acting as a Communications Provider (such as data identifying the destination for, or recipient of, an electronic communication), including for the following purposes: to route communications; for usage, billing, accounting, tax and compliance; to investigate wrongful or unlawful use of the Communications Network; to comply with Applicable Law and any other applicable laws and regulations (including any requests made by the UK's Information Commissioner's Office pursuant to Regulation 31A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR")); or to comply with the Agreement and Data Protection Addendum.

Communications Network: Public Switched Telephone Network (PSTN), Voice over Internet Protocol (VoIP) or other electronic communications network or service.

Communications Provider: a communications provider, as defined in section 405 of the Communications Act 2003.

Controller, processor, data subject, personal data, personal data breach, processing and **appropriate technical measures**: as defined in the Data Protection Legislation.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK, including: the Data Protection Act 2018 (and regulations made thereunder); UK GDPR, which has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018; and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

Supplier: IP Integration Limited.

Any other capitalised terms shall have the meaning set out in the Agreement.

2. Data protection

2.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause 2.1 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Legislation.

2.2 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the controller and the Supplier is the processor (except in relation to the Business Contact Information, in respect of which each party is an independent controller, and in respect of Communications Data, where the Supplier acts as an independent controller). Appendix 1 of this IPI Data Protection Addendum sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of personal data and categories of data subject.

2.3 Without prejudice to the generality of clause 2.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to the Supplier for the duration and purposes of the Agreement.

2.4 Without prejudice to the generality of clause 2.1, the Supplier shall, in relation to any personal data processed in connection with the performance by the Supplier of its obligations under the Agreement:

(a) process that personal data only on the documented written instructions of the Customer as set out in this IPI Data Protection Addendum and the Agreement, unless the Supplier is required by Applicable Laws to otherwise process that personal data. Where the Supplier is relying on Applicable Laws as the basis for processing personal data, the Supplier shall promptly notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Supplier from so notifying the Customer;

(b) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of

personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(c) ensure that all personnel who have access to and/or process personal data are obliged to keep the personal data confidential;

(d) not transfer any personal data outside of the UK, European Economic Area or other countries which do not have an 'adequacy' decision without notifying the Customer at least 30 days in advance and the following conditions being fulfilled:

(i) the Customer or the Supplier has provided appropriate safeguards in relation to the transfer;

(ii) the data subject has enforceable rights and effective legal remedies;

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any personal data that is transferred; and

(iv) the Supplier complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the personal data;

(e) assist the Customer, at the Customer's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(f) notify the Customer without undue delay on becoming aware of a personal data breach;

(g) at the written direction of the Customer, delete or return personal data and copies thereof to the Customer on termination of the Agreement unless required by Applicable Law to store the personal data; and

(h) maintain complete and accurate records and information to demonstrate its compliance with this clause 2 and allow for reasonable audits by the Customer or the Customer's designated auditor and immediately inform the Customer if, in the opinion of the Supplier, an instruction infringes the Data Protection Legislation.

2.5 The Customer consents to the Supplier appointing third party processors of personal data under this Agreement. The Supplier confirms that it has entered or (as the case may be) will enter with the third party processor into a written agreement substantially on that third party's standard terms of business and in either case which the Supplier confirms reflect and will continue to reflect the requirements of the Data Protection Legislation. As between the Customer and the Supplier, the Supplier shall remain fully liable for all acts or omissions of any third party processor appointed by it pursuant to this clause 2**Error! Reference source not found.**. A list of the Supplier's processors at the date of this Agreement is available at this link:
https://trust.ipiplatform.com/index.php/ipis-sub-processors/

Appendix 1

Processing, personal data and data subjects

1. Processing by the Supplier

1.1 **Subject matter of the processing:** The Supplier shall provide various Works as described in the Agreement.

1.2 **Duration of the processing:** The processing shall take place during the term of the Agreement and shall finish on termination or expiry of the Agreement, subject to each party's and their sub-processors' respective lawful data retention requirements.

1.3 **Nature and purpose of the processing:** Personal data may be provided by the Customer to the Supplier and/or its sub-processors in relation to the Works. For example, the Supplier may be providing a solution to the Customer, such as a workforce management system and / or a customer relationship management system, whereby the Customer's employees and / or end customers' data may be processed. Personal data may also be processed by the Supplier and / or its sub-processors in providing the relevant support.

Types of personal data: Full Name; Email Address; Telephone Number, and other types of personal data as further described at this link: https://trust.ipiplatform.com/index.php/ipis-sub-processors/

1.4 **Categories of data subject:** Customer's employees and other staff / end customers of the Customer (as applicable).

FAQs:

1. Why do we need to agree to the IPI Data Protection Addendum?

Many of IPI's services are 'multi-tenant,' which means that every customer needs to agree to the same data privacy provisions, while complying with GDPR. For example, given our multi-tenant offerings, we need to reserve the right to appoint third party processors to ensure the availability and stability of our platforms, including our ability to meet service levels for the benefit of all of our customers. This is why we require general written authorisation from our customers in relation to the appointment of sub-processors. We only onboard new processors once they've been vetted by our security and compliance team.

2. What drives your provisions in relation to data protection?

Cloud arrangements are based on a chain of sub-contractors (e.g. with the provider of SaaS reliant on the provider of PaaS, which in turn relies on an IaaS provider), and the lower-level providers (such as Amazon Web Services (AWS) and Microsoft Azure), which makes it extremely challenging to 'flow down' data protection obligations and liability terms in the way envisaged by GDPR.

3. Can I get a higher liability cap in relation to data protection?

If you require higher liability caps in relation to data protection, you could consider private cloud, rather than public cloud. However, this comes with disadvantages, including cost and resilience.

4. What other assurance can you provide?

IPI has direct obligations as a processor under UK GDPR / DPA 2018 to the ICO and to data subjects. IPI has robust security measures in place, along with various accreditations (such as ISO 27001 accreditation and the Cyber Essentials Certificate). Processing by IPI in third countries is generally limited to 'follow the sun' support, only after IPI has undertaken diligence including transfer impact assessments.