



innov8@comtrac.com.au | 1300 292 939

Master Terms & Agreements

Data Processing Agreement

INTRODUCTION AND GENERAL TERMS

Relationship with Comtrac's Master Services Agreement

This document forms part of the Comtrac Master Services Agreement (MSA). This document should be read in concert with all other documents which constitute Comtrac's MSA and other referenced material found at the Comtrac Trust Portal (<https://trust.comtrac.com.au>).

Definitions

In this document, unless the contrary intention appears, terms have the meaning given to them in the Comtrac Definition Schedule.

Compliance with Laws

Comtrac will comply with all Laws and regulations applicable to its provision of the Comtrac Services, including security breach notification Laws and Data Protection Requirements.

The parties acknowledge and agree that the Customer will act as the Data Controller in relation to the Processing of Personal Data, and Comtrac will act as the Data Processor, except where the Customer acts as a Processor of Personal Data, in which case, Comtrac is a sub-Data Processor.

When Comtrac acts as the Data Processor or sub-Data Processor of Personal Data, it will process Personal Data only on documented instructions of the Customer as detailed in the MSA or an Order Form. Any additional or alternate instructions must be agreed to in writing by the parties.

Scope

The terms in this **DPA** apply to all Comtrac Services that are provided by Comtrac to the Customer under the MSA.

Nature of Data Processing

Comtrac will use and otherwise process Customer Data and Personal Data only to provide the Customer the Comtrac Services in accordance with the MSA, and for Comtrac's legitimate business operations, pursuant to the terms of the MSA.

Processing to Provide Customer the Comtrac Services

When providing Comtrac Services, Comtrac will not use or otherwise process Customer Data or Personal Data for User Profiling, advertising or similar commercial purposes, or market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with the Customer's documented instructions.

Disclosure of Processed Data

For purposes of this section, "Processed Data" means Customer Data, Personal Data, and any other data processed by Comtrac in connection with the Comtrac Services, that is the Customer's Confidential Information.

Subject to any specific provisions of this MSA to the contrary, all processing of Processed Data is subject to Comtrac's obligation of confidentiality under the MSA. Comtrac will not disclose Processed Data except as the Customer directs, as described in this DPA or as required by Law.

Comtrac will not disclose Processed Data to law enforcement or other third parties unless required by Law. If Law enforcement contacts Comtrac with a demand for Processed Data, Comtrac will attempt to redirect the law enforcement agency to

request that data directly from the Customer. If compelled to disclose Processed Data to law enforcement or otherwise at Law, Comtrac will promptly notify the Customer (if it is permitted to do so) and provide a copy of the demand unless prohibited from doing so.

In support of the above, Comtrac may provide the Customer's basic contact information to the third party.

Processing of Personal Data - GDPR

All Personal Data processed by Comtrac in connection with the Comtrac Services is obtained as either Customer Data, Diagnostic Data, or Service Generated Data. Personal Data provided to Comtrac by, or on behalf of the Customer through use of the Comtrac Services is also Customer Data. Pseudonymised identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymised, or de-identified but not anonymised, or Personal Data derived from Personal Data is also Personal Data.

To the extent Comtrac is a Data Processor or sub-data processor of Personal Data subject to the GDPR, the GDPR Terms in PART B below govern that processing and the parties also agree to the following terms in this sub-section (**Processing of Personal Data - GDPR**).

Processing of Personal Data – GDPR Security Practices and Policies

Comtrac will implement and maintain appropriate technical and organisational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. Those measures shall be set forth in the Comtrac Information & Cybersecurity Standard. Comtrac will make that policy available to the Customer, along with descriptions of the security controls in place for the Comtrac Services and other information reasonably requested by the Customer regarding Comtrac security practices and policies.

Customer Responsibilities

The Customer is solely responsible for making an independent determination as to whether the technical and organisational measures for the Comtrac Services meet the Customer's requirements, including any of the Customer's security obligations under applicable Data Protection Requirements. The Customer acknowledges and agrees that (considering the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing of its Personal Data, as well as the risks to Individuals) the security practices and policies implemented and maintained by Comtrac provide a level of security appropriate to the risk with respect to the Customer's Personal Data.

The Customer is responsible for implementing and maintaining privacy protections and security measures for components that the Customer provides or controls (such as Customer Systems and Hardware, devices, including BYOD Devices), including hardware with Comtrac's software installed, and within the Customer's virtual machine or application.

Auditing Compliance

Comtrac will conduct audits of the security of the computers, computing environment and physical data centres that it uses in processing Customer Data and Personal Data, as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and
- Each audit will be performed by qualified, independent, third party security auditors at Comtrac's selection and expense.

Each audit will result in the generation of an audit report (**Comtrac Audit Report**), which will be Comtrac's Confidential Information and will clearly disclose any material

findings by the auditor. Comtrac will remediate issues raised in any Comtrac Audit Report to the satisfaction of the auditor. If the Customer reasonably requests (and only in circumstances where the findings of any Comtrac Audit Report are materially detrimental to the Customer's use of the Comtrac Services), Comtrac may provide the Customer with sufficient information for the Customer to assist in remediation of any risk.

Security Incident Notification

If Comtrac becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data or Personal Data while processed by Comtrac (each a **Security Incident**), Comtrac will promptly and without undue delay:

- Notify the Customer of the Security Incident;
- Investigate the Security Incident and provide the Customer with detailed information about the Security Incident; and
- Take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to the Customer's Security Representative by any means Comtrac selects, including via email. It is the Customer's sole responsibility to ensure that the Customer's management and administrators maintain accurate contact information for the Customer's Security Representative for notification purposes. The Customer is solely responsible for complying with its obligations under incident notification (**Mandatory Notifiable Data Breach**) Laws applicable to the Customer and for fulfilling any third-party notification obligations related to any Security Incident.

Comtrac shall make reasonable efforts to assist the Customer in fulfilling the Customer's obligation under GDPR Article 33 or other applicable Law or regulation to notify the relevant authority and Data Subjects about a Security Incident. Comtrac's notification of or response to a Security Incident under this MSA is not an acknowledgement by Comtrac of any fault or liability with respect to the Security

Incident. The Customer must notify Comtrac promptly about any possible misuse of its accounts or authentication credentials or any Security Incident or potential Security Incident related to the Comtrac Services.

DATA TRANSFERS AND LOCATION

Data Transfers

Except as described elsewhere in this DPA, Customer Data and Personal Data that Comtrac processes on the Customer's behalf may be transferred to, and stored and processed in, Australia or any other country in which Comtrac's service providers (sub-Data Processors) operate. The Customer appoints Comtrac to perform any such transfer of Customer Data and Personal Data to any such country and to store and process the Customer Data and Personal Data to provide the Comtrac Services as Comtrac elects. Where the Customer requires the Customer Data and Personal Data to remain only in Australia, it is the Customer's obligation to advise Comtrac in writing before the commencement of the MSA (data sovereignty within Australia is achievable through alternative sub-Data Processors).

All transfers of Customer Data out of the European Union, European Economic Area, and/or Switzerland by the Comtrac Services shall be governed by MSA to be entered into by the Customer and Comtrac.

Comtrac will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. All transfers of Personal Data to a third country or an international organisation will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

Location of The Customer Data at Rest

For the Customer Data held by Comtrac for the Comtrac Services, Comtrac will store Customer Data at rest within Australia or in a location explicitly requested, in writing

(on an Order Form) by the Customer and agreed to by Comtrac. Comtrac does not control or limit the regions from which the Customer or the Customer's Personnel may access or move Customer Data.

Data Retention and Deletion

At all times during the Term, the Customer will have the ability to create, read and update the Customer Data stored in and through the Comtrac Services.

Subject to termination of the Comtrac Services as provided for in the MSA and the relevant Order Form(s), Comtrac will retain Customer Data that remains stored in and through the Comtrac Services in a limited function account for 30 days after expiration or termination of the MSA so that the Customer may obtain the data in accordance with the clause of the MSA headed "Disengagement". After the 30 day retention period ends, Comtrac will disable the Customer's account and delete the Customer Data and Personal Data, unless Comtrac is permitted or required by Law, or authorised under this MSA, to retain such data.

The Comtrac Services may not support retention or extraction of software provided by the Customer.

Comtrac has no liability for the deletion of Customer Data or Personal Data as permitted under this MSA.

Processor Confidentiality Commitment

Comtrac will ensure that its Personnel engaged in the processing of Customer Data and Personal Data will process such data only on instructions from the Customer or as described in this DPA or as required for Comtrac to provide the Comtrac Services.

Comtrac shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to the Customer Data and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on Use of Sub-Processors

Comtrac may hire third parties to provide certain limited or ancillary services on its behalf as part of the Comtrac Services. The Customer consents to the engagement of these third parties and Comtrac service providers as sub-Data Processors. This constitutes the Customer's prior written consent to the subcontracting by Comtrac of the processing of Customer Data and Personal Data if such consent is required under the MSA or the GDPR Terms.

Comtrac is responsible for its sub-Data Processor's compliance with Comtrac's obligations in this DPA/MSA. When engaging any sub-Data Processor, Comtrac will ensure via a written contract that the sub-Data Processor may access and use the Customer Data or Personal Data only to deliver the services Comtrac has retained them to provide and is prohibited from using the Customer Data or Personal Data for any other purpose. Comtrac will ensure that sub-Data Processors are bound by written agreements that require them to provide at least the level of data protection required of Comtrac by the DPA.

From time to time, Comtrac may engage new sub-Data Processors. Comtrac will give the Customer notice of any new sub-Data Processor that is engaged and that materially impacts the Comtrac Services provided to the Customer, for example, where that sub-processor has access to Customer Data.

If the Customer does not approve of a new sub-Data Processor, then the Customer may invoke the Dispute Resolution process under the MSA.

PART B

European Union General Data Protection Regulation Terms

Comtrac makes the commitments in these GDPR Terms to the Customer. These commitments are binding upon Comtrac with regard to the Customer regardless of the Comtrac Services ordered. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Comtrac on behalf of the Customer. These GDPR Terms do not limit or reduce any data protection commitments that

Comtrac makes to the Customer elsewhere under the MSA. These GDPR Terms do not apply where Comtrac is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

Comtrac shall comply (to the extent it is required to) with Articles 23, 32 and 33 of the GDPR Terms.

Processing by Comtrac shall be governed by these Terms under European Union or its Member State law and are binding on Comtrac with regard to the Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of Data Subjects and the obligations and rights of the Customer are set forth in the MSA.