GDPR Position Statement

GENERAL PRIVACY AND DATA PROTECTION

1. Confidentiality

1.1. CT4 Pty Ltd (CT4) is committed to maintaining the highest degree of integrity in all our dealings with potential, current and past clients of CT4, both in terms of normal commercial confidentiality and the protection of all personal information received in the course of providing the business products and services provided by CT4.

1.2. CT4 extends the same standards to all of our clients, suppliers and associates. We will comply with the legislative requirements with regard to confidentially and data protection and will ensure all our sub-contractors and third-party suppliers (Sub Data Processors) agree and adopt our non-disclosure agreement and conditions for operating and processing our client data.

2. Ethics

2.1. We conduct our own services honestly and honourably and expect our clients (Data Controllers) and Sub Data Processors to do the same. Our advice, strategic assistance and the methods imparted through our services take proper account of ethical considerations.

3. Duty of Care

3.1. Through our actions and advice, we will always try to conform to relevant law and CT4 believes that all businesses and organisations, including our own business, have a duty of care to avoid causing any adverse effect on the rights and freedoms of individuals.

4. Terms and Conditions

4.1. Our contract and/or terms and conditions of engagement will usually be in the form of a detailed proposal, including aims, activities, costs, timescales and deliverables. They are supported by our General Data Protection Regulation (GDPR) statement of intent (see below) in respect of our processing activities as a Data Processor / Sub Data Processor under the GDPR.

4.2. The quality of our products and services and the value of our service to our clients are paramount to us and CT4 will always strive to meet our clients' contractual requirements. We shall ensure a compliance review is carried out against our own processing activities as a Data Processor / Sub Data Processor when supplying software products service solutions to our clients and ensure that all our Sub Data Processors do the same.

5. Intellectual Property & Moral Rights

5.1. CT4 retains the moral rights in, and ownership of, all intellectual property that we create unless agreed otherwise in advance with our clients. In return we respect the moral and intellectual copyright vested in our clients' intellectual property. Our suppliers are under strict terms of confidentiality not to disclose, disseminate and/or inform any third party about CT4’s clients, business or individual (data subjects) personal identifiable information.

6. Quality Assurance

6.1. CT4 maintains the quality of what we do through constant ongoing review with our clients, of all aims, activities, outcomes and the cost-effectiveness of every activity. We encourage regular review meetings and provide regular progress reports on the services we are engaged to deliver.

7. Professional Conduct

7.1. CT4 endeavours to conduct all of our activities with professionalism and integrity. We take great care to be completely objective in the judgement and any recommendations that are proposed, so that issues are never influenced by anything other than the best and proper interests of our clients.

GENERAL DATA PROTECTION REGULATION STATEMENT

1. Position Statement

This statement sets forth our approach with regard to compliance with our obligations under GDPR and related legislation in relation to:

(1) our products and services;

(2) as a Data Processor on behalf of our customers; and

(3) as a Data Controller of our employee data and promoting our products and services through marketing.

2. Data Processor

2.1. The role of the Data Processor is the processing of the data under the instructions of the Data Controller, (our clients). Under the GDPR, CT4 will:

(1) Provide software solutions which allow our clients, as Data Controllers, to process and store the Personal Identifiable Information (PII) of their data subjects.

(2) As a Data Processor, embed privacy principles in our approach when creating, designing a new, or maintaining an existing, software and/or storage solution.

(3) Where developing, designing, selecting and using applications, products and services that are based on the processing of personal data or the processing is necessary to fulfil a task, CT4, as a Data Processor, will take account of both the rights of individuals and the GDPR obligations of their clients as Data Controllers when developing and designing our products, services and applications. This will include performance of Privacy Impact Assessments (PIAs) with regard to our products and services for general application.

3. Data Controller

3.1. We understand that our clients, as Data Controllers, shall determine the means of processing as well as the risks of varying likelihood and severity for the rights and freedoms of an individual and in doing so they need to implement appropriate technical and organisational measures for security when it relates to PII as much as for pseudonymisation data sets.

3.2. Our clients, as Data Controllers, will be required to demonstrate compliance to adopt and implement measures which meet the Principles of data protection by design and data protection by default. Among other things, transparency will need to be demonstrated with regard to functions and to enable the individual (data subject) to monitor the data processing, enabling proper security controls are in place.

3.3. It is understood by CT4 that the role of the Data Controller is to ensure appropriate technical and organisational measures are in place to ensure and demonstrate compliance and are aware that as a Data Processor we need to support our clients as Data Controllers.

3.4. It is the Data Controller's responsibility to:

(1) ensure ongoing confidentially, integrity, availability and resilience of processing systems and services;

(2) restore and make available or accessible personal data in a timely manner in the event of a physical or technical incident; and

(3) regularly test and evaluate the effectiveness of the technical and organisational measures for security.

4. Data

4.1. Data is secured, and integrity and confidentiality are maintained, using technical and organisational means under the management of our client as a Data Controller when they position the software solution or product inside their own IT infrastructure.

4.2. When using CT4 data centre or storage services, CT4 may use the services of a third party which is as an EU based company and will act as a Sub Data Processor of CT4. When we use Sub Data Processors, CT4 will ensure full compliance required under the GDPR is observed as follows:

(1) Personal data will be processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Using appropriate technical or organisational measures (‘integrity and confidentiality).

(2) To support where applicable the responsibility and liability of a Data Controller in the requirement of responding to any risk or security assessments in regard to the processing of PII in relation to their data subjects.

5. Processing of Data

5.1. The processing of personal data is performed to the extent strictly necessary and proportionate for the purposes of ensuring network and information security.

5.2. Security is deemed to be the ability to resist accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data and the security of the related services offered by, or accessible via:

(1) networks and information systems;

(2) public authorities;

(3) emergency response teams and security incident response teams;

(4) service providers.

5.3. This includes preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to systems.

6. Pseudonymization

6.1. CT4 will assist its clients if they require a system configuration with regard to data encryption or pseudonymization.

7. Data Porting

7.1. Data Controllers must, where requested, supply an individual with a copy of their data in a structured, commonly used and machine-readable format and the individual has the right to ‘port’ that data without hindrance or delay. An individual has a right to require the Data Controller to transmit the data pertaining to them to another Data Controller where technically feasible.

7.2. CT4 will assist in supplying secure access or transmission solutions if the data porting applies to data we hold in our hosted environments.

8. Data Erasure

8.1. Our clients, as the Data Controller, will inform us as the Data Processor or Sub Processor where the right to rectification / erasure / restriction has been exercised by the individual. The exemption to this is if it involves disproportionate effort.

8.2. The Data Controller will inform the individual of all the recipients with whom their data has been shared will inform us as the Data Processor that such right has been exercised and the data subject’s PII is to be erased in any links to, or copies or replications of the personal data.

9. Data Breach

9.1. For the purposes of processing of PII which may result in a contravention of the GDPR (a data breach), CT4, as the Data Processor, and/or our Sub Data Processors, will determine if

(1) a breach is likely; and

(2) there is a high risk to processing of the PII in the systems held outside of our clients IT infrastructure (e.g. hosted by our third party Sub Data Processors,) which could put at risk the rights and freedoms of data subjects

9.2. CT4 will ensure such technical measures are in place to identify, track, assess and report data breaches. We will report all contraventions with regard to data security to our clients as Data Controllers.

9.3. Where our client requires us as the Data Processor or our Sub Data Processor to carry out activities which could lead to a contravention of GDPR, we as Data Processor and our Sub Data Processors reserve the right to refuse such processing activities to address the reporting obligations to the individual (data subject) as well as to the Information Authority in the member state where the data is held and processed.

10. Engagement of Sub Data Processors and Contractual Obligations

10.1. As Data Processor, CT4 shall not engage a Sub Data Processor without specific or a general written authorisation of our clients as Data Controllers.

10.2. Where CT4 and/or the client as a Data Controller require services from a Sub Data Processor, each will consult and require demonstration of compliance under the GDPR by the Sub Data Processor. This will be in writing and each party will demonstrate compliance and record such in the contract and record any intended changes concerning the engagement, replacement or addition of a Sub Data Processor allowing time for the parties to object and/or agree.

10.3. The relationship between our clients as Data Controllers and CT4 as the Data Processor and our Sub Processors will be governed by a contract that is binding on the Data Processor / Sub Processor.

10.4. The contract will set out, as a minimum:

(1) the subject matter;

(2) duration;

(3) the nature and purpose of the processing;

(4) the types of personal and sensitive categories of data; and

(5) the categories of data subjects;

(6) the obligations and rights of the Data Controller;

10.5. The contract shall provide, in particular, that the Data Processor and any Sub Data Processors:

(1) only process data on documented instructions from the Data Controller;

(2) do not transfer any personal data to a third country or international organisation, unless required to do so by European Union or Member State law to which the Data Processor and/or Sub Data Processors are subject (in these circumstances the Data Processor shall inform the Data Controller of such legal requirement before processing, unless the law prohibits such information on important grounds of public interest);

(3) ensure that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(4) take measures to secure personal data;

(5) ensure the Sub Data Processor follows the same contractual conditions and obligations as the main Data Processor and in doing so is liable under the same contractual agreements for any breach of such agreement;

(6) provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR.

(7) assist the Data Controller in a timely manner in all matters pertaining to the response and processing of data with regard to data subjects' rights;

(8) assist the Data Controller by:

(a) ensuring data is kept secure;

(b) notifying the Data Controller of any potential or actual breach;

(c) assisting the Data Controller with any information to inform any affected individual;

(9) work with the Data Controller with regard to any consultation with the Information Authority;

(10) are permitted the right to inform the Data Controller if, in their opinion, an instruction from the Data Controller infringes GDPR or other European Union or Member State data protection provisions.

10.6. CT4 as the Data Processor will not make any determination of the use of their clients' PII, as in doing so it would mean we would be considered to be a Data Controller.

11. Liability and Right to Compensation

11.1. CT4 as the Data Processor shall be liable for the damage caused by the processing only where it has not complied with the obligations of the EU GDPR, Union and Member State Law.

11.2. CT4 as Data Processor shall be exempt from liability if we can prove that we are not in any way responsible for the event giving rise to the damage.

11.3. Either jointly or severally, both the Data Controller and the Data Processor can be found liable for the entire damage in order to ensure effective compensation of the data subject affected.

11.4. Where the CT4 as Data Processor has paid full compensation for the damage suffered, we are entitled to claim back from the Data Controller or other Data Processor that part of the compensation corresponding to their part in the responsibility for the damage.