General Data Protection Policy

Ingenium Training and Consulting Ltd. (Ireland)

1. Interpretation

1.1 Definitions:

Company (we/our/us): Ingenium Training and Consulting Limited, a company registered under the laws of Ireland under company number 555643 with its main operating premises at No. 68 O'Connell Street, Limerick, Ireland.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, and members of the Company.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with Data Protection Law. The Company is the Controller of all Personal Data relating to Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data. In this policy, Data Subjects referenced are Company Contacts, as defined.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Law: means all legislation and regulations relating to the protection of Personal Data including (without limitation) the Data Protection Acts 1988-2018, the GDPR and all other statutory instruments, industry guidelines (whether statutory or non-statutory) or codes of practice or guidance issued by the Data Protection Commission relating to the processing of personal data or privacy or any amendments and re-enactments thereof.

Data Protection Contact: the person appointed by the Company to manage with its Data Protection Law compliance framework, namely Alan Higgins – alan.higgins@ingeniumtc.com.

GDPR: the General Data Protection Regulation (GDPR) (EU) 2016/679.

Personal Data: means any information from which a Data Subject can be identified, whether directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Law.

Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: all other policies, operating procedures or processes the Company has in place to ensure the protection of Personal Data.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.
Third Country: Country outside the European Economic Area.

2. Introduction

This Data Protection Policy sets out how the Company is required to handle the Personal Data of its customers, clients, suppliers and other third parties who may engage with the Company for various reasons (excluding employees), (hereinafter collectively referred to as "Company Contacts") in order to comply with Data Protection Law

This Policy should be read in conjunction with the Company's Privacy Policy.

This Data Protection Policy applies to all Personal Data of Company Contacts we Process, regardless of the medium via which it is collected or stored and regardless of whether it relates to past, present or potential Company Contacts.

Company Personnel are required to read, understand and comply with this Data Protection Policy when Processing Personal Data on the Company's behalf.

3. Scope

We recognise that correct and lawful treatment of Personal Data will maintain confidence in the Company and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Depending on the nature of the breach, the Company is exposed to potential fines of up to €20 million or 4% of total worldwide annual turnover, whichever is higher, for failure to comply with the provisions of the GDPR.

Each of the Company's officers are responsible for ensuring the Company's compliance with all aspects of Data Protection Law and the officers have appointed the Data Protection Contact to implement and oversee the necessary policies and procedures which form an integral part of this compliance.

Any Company Contacts with any questions or concerns in relation to how their Personal Data is handled by the Company, to include concerns regarding compliance or alleged non-compliance with this Data Protection Policy, should get in touch with the Data Protection Contact.

4. Personal data protection principles

The Company strives in carrying out its day-to-day functions to adhere fully to the principles relating to Processing of Personal Data as set out in Data Protection Law which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes.

Data Protection Law restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

Data Protection Law allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests;
(e) to pursue our legitimate interests; or
(f) processing is necessary for the performance of a task carried out in the public interest.

The Company must identify and document the legal ground being relied on for each Processing activity.

Where Special Categories of Personal Data are Processed by the Company, different legal grounds for Processing apply.

For specific information in this regard, Company Contacts should refer to our Privacy Policy.

6. Consent

As set out in section 5 of this policy, a Controller must only process Personal Data on the basis of one or more of the lawful bases set out in Data Protection Law. In certain circumstances Consent may be the basis relied upon.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

Where consent is the lawful basis for processing, Data Subjects must be easily able to withdraw such Consent at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Where Consent is relied on to Process Cookies via the Company's website, Consent is only valid for a 6 month period.

The Company is required to evidence Consent captured and keep records of all Consents in accordance with Related Policies so that it can demonstrate compliance with Consent requirements.

7. Transparency (notifying Data Subjects)

Data Protection Law requires Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with all the information required by Article 13 of the GDPR, including the identity of the Controller and Data Protection Contact, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party), we must provide the Data Subject with all the information required by Article 14 of the GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with Data Protection Law and on a basis which contemplates our proposed Processing of that Personal Data.

For specific information in this regard, Company Contacts should refer to our Privacy Policy.

8. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. As a general rule it must not be further Processed in any manner incompatible with those purposes.

Personal Data cannot be used for new, different or incompatible purposes from that disclosed when it was first obtained unless (1) the Data Subject has been informed of the new purposes and have Consented where necessary, or (2) such Processing is in line with the permitted exemptions to the purpose limitation rule as provided for in the Data Protection Act 2018 for e.g. to defend a legal claim or to take legal advice.

9. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

The Company must not Process Personal Data beyond the timeframe for which it is required for the purpose it was collected, unless it is required for a different, permitted purpose (please refer to section 8) or, unless the Company is required by some legal or regulatory obligation to retain such Personal Data.

All Personal Data processed by the Company is confidential and must be treated as such by Company Personnel. Company controlled Personal Data must not be disclosed to any third party save where required by law or as set out in the Company Privacy Policy.

The Company is required to ensure any and all Personal Data collected by it via Company Personnel is accurate, adequate and relevant for the intended purposes. Excessive Personal Data beyond what is required should not be collected.

Where the Company no longer has a lawful basis to Process Personal Data of Data Subjects, that Personal Data will be securely deleted or destroyed (per section 11 below).

10. Accuracy

Personal Data must be accurate, complete, kept up to date and relevant to the purpose for which we collect it. Where a Data Subject becomes aware that any Personal Data Processed by the Company about them is inaccurate, this should be brought to the attention of the Data Protection Contact (or a Company employee, who will then refer the request on to the Data Protection Contact) without delay.

Save for exceptional circumstances as provided for by Data Protection Law, Personal Data will be corrected as soon as possible.

11. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company is required to maintain policies and procedures which ensure Personal Data is deleted after a reasonable time from the expiration of the purposes for which it was being held, unless a law or other regulation to which the Company is subject, requires that data to be retained by the Company.

The Company will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete that data where applicable.

12. Security integrity and confidentiality

12.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain technical and organisational safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we control and any identified risks.

Personal Data should only be shared with third-party service providers with whom there is a data processing agreement in place (ensuring the continued security and protection of Company-controlled Personal Data), as required pursuant to Article 28 of the GDPR.

12.2 Reporting a Personal Data Breach

Pursuant to Data Protection Law Controllers are required to notify a Personal Data Breach to the Data Protection Commission no later than 72 hours after the breach. Where the Personal Data Breach is likely to result in a high risk to the affected individuals, organisations must also inform those affected individuals of the breach without undue delay.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

13. Transfer limitation

Data Protection Law restricts the transfer of Personal Data to a Third Country. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

Third Country Personal Data transfers are lawful only if one of the following conditions applies:

(a) the European Commission has deemed that the said country has an adequate level of protection for the Data Subject's rights and freedoms (an adequacy decision);
(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses adopted and approved by the European Commission or an approved code of conduct or a certification mechanism;
(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(d) the transfer is necessary for one of the other reasons set out in Chapter 5 of the GDPR, including the performance of a contract between the Company and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

14. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time (where the Company relies on consent to Process Personal Data);
(b) receive certain information about the Controller's Processing activities;
(c) request access to Company-controlled Personal Data;
(d) prevent our use of Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) object to the Processing of your Personal Data by the Company;
(i) be notified of a Personal Data Breach which is likely to result in a high risk to your rights and freedoms;
(j) make a complaint to the Data Protection Commission;
(k) Bring a civil litigation claim for breaches of Data Protection Law by the Company vis-à-vis your Personal Data irrespective of whether material damage has occurred; and
(l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

Rights requests should be exercised via the Data Protection Contact only.

A number of the rights provided for above have a time limitation for responding, the most frequent of which is 30 days.

Some of the above rights are not absolute and if for any reason the Company cannot comply with a rights request, a Data Subject should be given full information and reasons for such non-compliance.

15. Accountability

The Company as Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. It is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company should have adequate resources and controls in place to ensure and to document compliance with Data Protection Law, including:

(a) appointing an individual to deal with data protection compliance internally;
(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
(c) integrating data protection into internal documents including this Data Protection Policy and Related Policies or Privacy Notices;
(d) regularly training Company Personnel on Data Protection Law, this Data Protection Policy, Related Policies and general data protection matters including, for example, Data Subject's rights, Consent, legal bases for processing, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16. Record keeping

Data Protection Law requires Controllers to keep full and accurate records of its data Processing activities. This includes records of Data Subjects' Consents and procedures for obtaining Consents as well as (i) the name and contact details of the Controller and the Data Protection Contact, and (ii) clear descriptions of the types of Personal Data processed by it, Data Subject types, Processing activities,

Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

A copy of the Company's records are available via request to the Data Protection Contact.

17. Data Protection Impact Assessment (DPIA)

Where Personal Data Processing by the Company involves a particularly high risk to the rights and freedoms of Data Subjects, the Company will conduct a DPIA before engaging in the particular Processing activity. Examples of Processing which may require a DPIA:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling;
- large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA should include:

- a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

18. Direct marketing

We are subject to the ePrivacy Regulations (S.I. 336/2011) (as may be amended from time to time), as well as Data Protection Law when marketing to our customers.

The general rule for electronic direct marketing (marketing via email, text, fax, telephone) is that it requires the affirmative consent of the recipient (such as by specifically opting-in) under Regulation 13 of the ePrivacy Regulations (SI 336/2011). Even where a direct marketer has the consent of a data subject, that consent may be withdrawn by the data subject, and in all cases of direct marketing, under Article 21 GDPR the data subject has the right to object at any time to the use of their personal data for such marketing, which includes profiling related to such direct marketing.

The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

If you receive marketing material from us which you do not wish to receive, you should make this known to the Data Protection Contact who will unsubscribe you from such communications immediately.

19. Sharing Personal Data

As a general rule, the Company will not share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

The Company will only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d) the transfer complies with any applicable cross-border transfer restrictions; and
(e) a fully executed written contract is in place with that third party, as required pursuant to Article 26 or Article 28 of the GDPR.

In certain limited circumstances, the Company may share Personal Data with third parties without having an opportunity to implement some/all of the foregoing safeguards for e.g. sharing information with An Garda Síochána, our insurers or our lawyers where an incident has taken place which requires immediate investigation.

20. Changes to this Data Protection Policy

This Data Protection Policy may be amended from time to time and the latest version will be available via our website, http://ingeniumtc.com/ or via request to the Data Protection Contact.