Data Protection Policy

July 2024

Version No	Date Issued	Update Details	Owner	Approved by	Policy Number
v3.0	February 2022	Policy in previous format	Company Secretary	The Board	CG1-POL-014
v4.0	August 2023	Policy finalised following revision and review of February 2022 policy, amendments and change of format.	Company Secretary	The Board	CG1-POL-014
v4.1	July 2024	Policy reviewed, minor changes of format.	Head of Internal Investigations (DPCO)	The Board	POL-014

Data Protection Policy

Everyone has rights in respect of how their personal information is handled. We recognise the need to treat everyone's Personal Data in an appropriate and lawful manner pursuant to the General Data Protection Regulation (GDPR), the UK GDPR (the GDPR as it forms part of the law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act of 2018) and Data Protection Act 2018.

Policy

Clancy Group Holdings Limited and its subsidiaries (Clancy or we) have set out in this policy how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties. It also sets out the rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation, and destruction of personal data.

This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

This policy is reviewed regularly by the Head of Internal Investigations (GDPR & DPA Compliance Officer) and will be monitored for compliance by Line Managers/Supervisors within their own area of responsibility. If you have any questions or concerns at any time around any matters covered, possibly covered, or in relation to the day-to-day application of this policy, speak to the Head of Internal Investigations (GDPR & DPA Compliance Officer).

This policy does not form part of any contract of employment or other contract to provide services and we may amend it at any time.

Definitions

Criminal Convictions Data: Personal Data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Consent: agreement which must be freely given, specific, informed, and is 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.

Data: information, which is stored electronically, on a computer, or in paper-based filing systems.

Data Subjects: all living individuals about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights in relation to their Personal Data.

Personal Data: any information identifying a Data Subject or information relating to Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal Data can be factual (such as a name, address, date of birth, location or other descriptors) or it can be an opinion (such as a performance appraisal). A name is not always necessary. For example, other identifiers such as IP address, cookies, radio frequency identification tags (RFIDs) are all considered to be Personal Data where an individual can be identified as a result of their use.

In addition, any two or more pieces of data that together identify an individual are considered to be Personal Data. Identification may be by any means reasonably likely to be used. Personal Data excludes anonymous data or data that has had the identity of an individual permanently removed.

Data Controller: the person or (more usually) organisations that determine when, why and how to process Personal Data. They have a responsibility to establish practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data used in our business.

Data Users: individuals (including employees) whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data Processors: individuals who handle data on behalf of a Data Controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Data Protection Officer (DPO): voluntary appointment of a DPO with responsibility for data protection compliance.

Processing or Process: any activity that involves 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, storing, reading, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

Special category Personal Data: includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric information, health and sexual life or sexual orientation. 'Special category' or 'sensitive' Personal Data may not be processed unless certain strict conditions are met and will frequently require the express consent of the individual concerned.

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Who must comply with this policy?

This policy applies to all employees working for Clancy at all levels and also applies to consultants, seconded employees, agency workers, agents, or any other person associated with Clancy, (referred (referred to as “you” in this policy).

You must read, understand and comply with this policy when Processing Personal Data on our behalf. This policy sets out what we expect from you for Clancy to comply with applicable law. Your compliance with this policy is mandatory.

Accountability

Ultimately, it is your responsibility and the responsibility of all Data Controllers to minimise the risk of breaches and to protect personal data. You must familiarise yourself with internal processes and procedures to ensure compliance with this policy.

We must have adequate resources and controls in place to ensure and to document UK GDPR compliance. To comply with the requirements of governance and accountability, we have:

- implemented technical and organisational measures to ensure and demonstrate that we comply with data protection principles. This includes developing new policies and regularly reviewing existing internal policies, employee training on the UK GDPR, this policy and our privacy notices. We also conduct internal audits of processing activities to assess compliance, including using results of testing to demonstrate compliance improvement effort;

- produced a register of personal information, the purpose of processing, the lawful basis for processing and retention schedules;

- appointed an external DPO (or nominated person);

- implemented Privacy by Design when processing Personal Data, Measures we may use include data minimisation, pseudonymisation and transparency;

- committed to a process of improvement to ensure that we continuously assess our working practices to ensure that we comply with best practice; and

- implemented a process of mandatory Data Protection Impact Assessments (DPIAs) where processing presents a high risk to rights and freedoms of Data Subjects for example, where new suppliers are engaged, when implementing major system or business change programs (involving the Processing of Personal Data including the use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

Information we may handle

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, clients, advisors, stakeholders and others who we communicate with. We must protect personal information wherever it is held within Clancy, including on paper, computer or other media.

Data Protection Officer

The DPO or nominated person is responsible for:

- ensuring that we adhere to the principles of the UK GDPR;
- ensuring that you have received adequate data protection training;
- monitoring data protection documentation and procedures to ensure compliance with the UK GDPR;
- ensuring that any request to exercise data subject rights under the UK GDPR submitted by an individual is handled in accordance with Clancy's Individual Rights Policy and related processes; and
- ensuring that our data protection records are correct, valid and up to date.

Some of the responsibilities set out above may be delegated by the DPO or nominated person, provided formal reporting and lines of communication are in place to ensure the DPO, or nominated person retains adequate oversight of UK GDPR-related activities.

UK GDPR Principles

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

b) collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

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;

e) kept in a form which permits identification of Data Subjects for no onger than is necessary for the purposes for which the data is Processed (storage limitation);

f) processed in a manner that ensures appropriate security of the Personal Data using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality); and

g) made available to Data Subjects and allow them to exercise certain rights in relation to their Personal Data (Data Subject's rights and Data Subject Access Requests ("DSAR").

Whenever we collect Personal Data, the Data Subject must be told:

- who the Data Controller is (in this case Clancy);
- how to contact the Data Controller's representative (in our case, the DPO, or nominated person);
- the purpose for which the data is to be processed; and
- the information regarding third party recipients (for example, suppliers) to whom the data may be disclosed or transferred.

Lawfulness, fairness and transparency

We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR 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.

The UK GDPR specifies the grounds (conditions) that can be used for lawful processing, some of which are set out below:

a) **consent:** demonstrated by the Data Subject performing a clear affirmative action (for example, ticking an opt-in box);

b) **contract:** processing is necessary for the performance of a contract with the Data Subject;

c) **legal obligation:** processing is necessary to comply with the law (not including contractual obligations);

d) **vital interests:** the processing is necessary to protect an individual's life;

e) **public task:** the processing is necessary to perform a task in the public interest or for your official functions; and

f) **legitimate interests:** The processing is necessary to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

Transparency (notifying Data Subjects)

The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice 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 a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and 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 or publicly available source), we must provide the Data Subject with all the information required by the UK 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 the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice. You should discuss any existing or new Privacy Notices with the Legal Counsel.

Consent

A Data Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which includes Consent.

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. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Personal Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than explicit consent or Consent if possible.

Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share Personal Data we hold with another employee, agent or representative of Clancy if the recipient has a job-related need to know the information.

You may 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 that contains UK GDPR-approved third party clauses has been obtained.

Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. This means that Personal Data must not be collected for one purpose and then used for another.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO or Company Secretary for advice on how to do this in compliance with both the law and this Data Protection Policy.

Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. Personal Data must only be collected to the extent that it is required for the specific purpose notified to the Data Subject. Any Personal Data which is not necessary for that purpose must not be collected in the first place.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties. Do not collect excessive data. You must ensure that any Personal Data collected is adequate and relevant for the intended purposes.

Accurate data

Personal data must be accurate and, where necessary, kept up to date. Information which is incorrect or misleading must be corrected or deleted without delay when inaccurate. Where a Data Subject disputes the accuracy of their Personal Data, the disputed data must be flagged until the dispute is resolved.

You must ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data

at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

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. This means that data must be destroyed or erased from our systems when it is no longer required.

We maintain retention policies and procedures to ensure that Personal Data is deleted after an appropriate time unless a law requires that data to be kept for a minimum time. You must comply with Clancy's Records Management Policy.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

For guidance on how long certain data must be kept before being destroyed, refer to the Records Management Policy, or contact the Company Secretary or nominated person.

Direct Marketing

We are subject to certain rules and privacy laws when engaging in direct marketing to our clients and prospective customers (for example when sending marketing emails or making telephone sales calls).

A Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls).

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 always be promptly honoured. If a client opts out of marketing 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.

Security integrity and confidentiality

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 safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable).

We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold.

You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

b) integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

c) availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

Transfer limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. 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.

We are required to ensure that adequate safeguards are in place if it is necessary to transfer Personal Data outside of the UK. This includes granting access to our Personal Data by suppliers and business partners and other organisations in Clancy that may be located in countries outside of the UK who are not approved by the Data Protection authorities as having equivalent (adequate) data protection laws in place to protect the rights of individuals.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

b) appropriate safeguards are in place such as standard contractual clauses approved for use in the UK;

c) the transfer is necessary for one of the other reasons set out in the UK GDPR including:
   i. the performance of a contract between us and the Data Subject;
   ii. reasons of public interest;
   iii. to establish, exercise or defend legal claims;
   iv. to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
   v. in some limited cases, for our legitimate interest.

Data Subject's access rights and requests

A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Controller's Processing activities;

c) request access to their Personal Data that we hold;

d) prevent our use of their 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) request a copy of an agreement under which Personal Data is transferred outside of the UK;

i) object to decisions based solely on automated Processing, including profiling by automatic decision making;

j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

l) make a complaint to the supervisory authority; and

m) 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;

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

Fulfilment of Data Subject access rights and requests

We have implemented formal processes for dealing with requests to exercise the above rights.

You must notify the Head of Internal Investigations (GDPR & DPA Compliance Officer) immediately if a Data Subject wishes to request a copy of the Personal Data held about them or makes a request to exercise any of the other above rights.

Requests received over the telephone must be made in writing by the Clancy employee and forwarded immediately to the Head of Internal Investigations for processing.

Data Subjects are entitled to receive copies of any Personal Data we hold within one calendar month of receipt by Clancy and all functional departments are required to support the Head of Internal Investigations in locating the Personal Data requested as a matter of urgency.

If you are an existing employee, you may contact HR to request copies of your Personal Data should you wish to do so. HR will continue to handle such requests as part of routine HR administration where they are able to. This does not prevent existing employees from submitting a formal (written) DSAR, in which case, the request must be forwarded to the Head of Internal Investigations.

Reporting a Personal Data Breach

Security incidents, events (near misses) and weaknesses must be reported to the IT Helpdesk immediately.

The UK GDPR requires Data Controllers to notify any Personal Data breach to the ICO 72 hours of becoming aware and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Head of Internal Investigations. You should preserve all evidence relating to the potential Personal Data breach.

Refer to the Data Breach and Incident Management Policy for more information.

Legal liability

We are exposed to potential fines of up to 4% of total worldwide annual turnover depending on the breach for failure to comply with the provisions of the UK GDPR.

Alternatively, the ICO has powers to issue an enforcement notice or an information notice where a Data Controller has failed to comply with any of the data protection principles. Failure to comply with such a notice is an offence and we could be fined and/or individual employees (including directors of Clancy) may be subject to criminal proceedings.

You must be aware that it is an offence to unlawfully obtain or sell (or offer to sell) Personal Data. You must:

- not access or use Clancy Personal Data without authorisation;
- only use Personal Data in performance of your official duties;
- not use Personal Data for your own purposes, however well-meaning your intentions;
- not share or disclose Personal Data to anyone not entitled to have it, including Personal Data relating to colleagues;
- not knowingly or recklessly, re-identify anonymised Personal Data; and
- not intentionally attempt to destroy or tamper with Personal Data to avoid its disclosure to the data subject when a DSAR is received.

Training

We are required to ensure all Staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
You must undergo all mandatory data privacy-related training and ensure your team undergoes the same or similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Breach of this policy

If you breach this policy, you may face disciplinary action which could result in dismissal for misconduct or gross misconduct in accordance with our Disciplinary Policy. In addition, we may refer the matter to the ICO, and law enforcement bodies where warranted. We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.