

The Clancy Group Plc Policy Statement



PRIVACY POLICY

Policy Statement

The Clancy Group Plc its subsidiaries and/or associated companies (Clancy) is one of the largest privately-owned construction firms in the UK with almost 60 years' experience with a large workforce.

We are committed to protecting your personal information, as well as being transparent about the personal information collected, obtained and disclosed about you. This Privacy Policy relates to our use of the personal information we collect from you via the Clancy websites. It is possible to access all of Clancy's website pages without having to provide any personal data.

Processing of personal data, such as name, address, email, IP address or telephone number by Clancy shall be in line with the General Data Protection Regulation (GDPR), the UK Data Protection Act (DPA) and in accordance with all country-specific data protection regulations applicable to Clancy. By means of this data protection declaration, Clancy would like to inform you of the nature, scope and purpose of the personal data we collect, use and process. Furthermore, you are informed, by this declaration, of the rights to which you are entitled.

The Board of The Clancy Group Plc has approved this policy.

Scope

This Policy applies to all permanent, temporary and contracted employees working for and on behalf of Clancy.

Personal Data Collected By Clancy

Clancy collects a range of personal information about you, which may include, but is not limited to:

- Name, address and contact details, including email address and telephone number;
- Sex/gender;
- Age/date of birth;
- Copy of driving licence and / or passport / identity card;
- National insurance number and other tax-related information;
- Details of employment history, experience;
- Information relating to entitlement to work in the UK;
- Details of any criminal convictions; and
- CCTV footage, if attending our premises.

Clancy collects this information in a variety of ways, for example, data contained within an application form/CV, obtained from your passport or other identity documents or collected through interviews. Information will also be collected from third parties, such as references supplied by former employees.

Clancy will store your personal data securely, in a number of locations, including on Clancy sites and IT systems (including email and servers).



Safe. Successful. Sustainable. Secure. Skilled. Systems.



Name And Address Of Clancy

For the purposes of the GDPR, DPA or other country-specific data protection laws and other provisions related to data protection, the data controller is:

The Clancy Group Plc
Clare House
Coppermill Lane
Harefield
Middlesex
UB9 6HZ

Phone: 01895 823711
Email: enquiries@theclancygroup.co.uk

Name And Address Of Data Protection Officer

Data Protection Officer
The Clancy Group Plc
Clare House
Coppermill Lane
Harefield
Middlesex
UB9 6HZ
United Kingdom

Phone: 01895 823711
Email: DPOfficer@theclancygroup.co.uk

You may, at any time, contact our Data Protection Officer, or nominated person with all questions and suggestions concerning data protection.

Cookies

Clancy websites use cookies for making your visits to our websites more efficient. Please see our Cookies Policy for further information.

Collection Of General Data And Information

Clancy collects a range of general data and information when users visit the websites. This general data and information are stored in our server log files and include:

- The browser types and versions used;
- The operating system used by the accessing device;
- The website from which an accessing device reaches our website (so-called 'referrers') such as Google;
- The date and time of access to the website;
- The Internet protocol address (IP address) used to access the website;
- The Internet service provider of the accessing device, and
- Any other relevant data and information that we deem vital to preventing malicious attacks on our information technology systems or for troubleshooting our information technology systems in the event of any malicious attack, real or perceived.



Safe. Successful. Sustainable. Secure. Skilled. Systems.



Clancy does not draw any conclusions about individual users when processing or analysing this general data and information. This information is needed to:

- Deliver the content of our website correctly;
- Optimise the content of our website as well as its advertisement;
- Protect the long-term viability of our information technology systems and website technology; and
- Provide law enforcement authorities with the information necessary for criminal prosecution in case of a cyber-attack or criminal misuse.

In light of this, Clancy analyses collected data and information statistically and in the aggregate, with the aim of increasing the data protection and data security of our Company and to ensure an optimal level of protection for the personal data we process. The data of the server log files are stored separately from any personal data provided by users.

Security

The security of personal data is important to us. We regularly monitor our systems for possible vulnerabilities and attacks, and we use reasonable organisational, technical and administrative measures to protect personal data under our control. Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us of the problem by contacting our Data Protection Officer.

Sharing Your Personal Information With Clancy

You may submit your personal data for a variety of reasons, for example, to subscribe to Clancy Plant newsletters. The personal data provided by you is collected and stored exclusively for internal use.

Disclosure Of Your Personal Data

Information provided to Clancy may be shared with the following:

- Internally with Clancy employees, contractors and suppliers who provide services on behalf of Clancy;
- Clancy solicitors and other advocacy partner organisations;
- Insurers;
- Clancy professional advisors;
- Providers of IT and system administrative services; and
- Public bodies and regulatory authorities.

Clancy will not share your personal data with any organisations in return for payment.

Rights To Access And Control Your Personal Data

You have a legal right to access personal information Clancy holds about you, including the right to:

- Be informed how your personal information is processed;
- Have inaccurate or incomplete personal data rectified;
- Access a copy of the personal data Clancy holds on you;
- Restrict the processing of your personal data, in certain circumstances, e.g. if you have challenged the accuracy of your data;



Safe. Successful. Sustainable. Secure. Skilled. Systems.



- Object to the processing of your personal data for marketing purposes;
- Receive a copy of your personal data, in a machine-readable format, for your own personal use or to transfer to another organisation;
- Have your personal data erased, in those circumstances where there is no compelling reason for Clancy to continue processing it, insofar as there are no statutory storage obligations;
- Claim compensation for damages caused by a breach of data protection laws; and
- Withdraw your consent, at any time.

Clancy does not use automated decision making to make decisions.

Contacting Clancy Via The Website

If you contact Clancy via email, the personal data transmitted by you is automatically and securely stored on access-restricted Clancy servers. Such personal data transmitted on a voluntary basis by you to Clancy is stored for the purpose of processing or contacting you. There is no transfer of this personal data to third parties.

Data Protection For Job Applications And The Application Procedures

Clancy collects and processes personal data of job applicants, including apprenticeships and graduate schemes in accordance with Clancy's application procedure. Processing will be carried out electronically when an applicant submits corresponding application documents to the Clancy recruitment email address Recruitment@theclancygroup.co.uk

If your application is successful, the personal data submitted will be stored for the purpose of processing the employment relationship in compliance with legal requirements. The data will be transferred to your personnel file and retained for the duration of your employment at Clancy and 6 years post-employment.

If your application for employment is unsuccessful, Clancy's Recruitment Team will seek your consent to hold your personal data on file for up to 6 months after the recruitment process. If consent is provided, paper copies of your data will be securely destroyed and securely deleted after the 6 months has lapsed.

Lawful Basis For The Processing

The GDPR/DPA or country-specific data protection regulations applicable to Clancy set out the lawful basis for processing personal data. Processing of personal data may be necessary for contract purposes, for example, for the supply of goods or to provide any other service. The same applies to such processing operations, which are necessary for conducting pre-contractual measures, for example in the case of enquiries concerning our products or services.

Clancy is subject to a legal obligation by which processing of personal data is required, such as for the fulfilment of tax obligations. In rare cases, the processing of personal data may be necessary to protect the vital interests of you or of another natural person. For example, if a visitor were injured on a Clancy site, their name, age, health insurance data or other vital information may need to be passed on to a doctor, hospital or other third party.

Processing not covered by any of the above-mentioned legal grounds, may be necessary for the purposes of the legitimate interests pursued by Clancy, except where such interests are overridden by your interests or fundamental rights and freedoms, which require protection of personal data. Such processing operations are permissible if they have been specifically mentioned and are in accordance with the country-specific data protection regulations applicable to Clancy. It is considered that a legitimate interest could be assumed if you or your employer are a Clancy client. We will always seek your consent prior to using your data for any purpose that is not covered by another lawful basis.



Safe. Successful. Sustainable. Secure. Skilled. Systems.



The Legitimate Interests Pursued By Clancy

The processing of personal data to carry out our business in favour of the well-being of all our employees is considered a 'Legitimate Interest Pursued by Clancy'.

Period For Which The Personal Data Will Be Stored

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfilment of a contract or the initiation of a contract.

Cross-Border Transfer

Where Cloud-based applications or storage are used, we may transfer data to countries outside of European Economic Area (EEA). We will make every effort to ensure that data remains in the EEA, but it is possible that data will be transferred to countries, which may have data protection rules that are different to those of your country. However, we will ensure that any such transfers comply with applicable data protection laws and that your data remains protected to the standards described in this Privacy Policy. In certain circumstances, courts, law enforcement agencies, regulatory agencies or security authorities in those other countries may be entitled to access your personal data for legal requirements.

Provision Of Personal Data As Statutory Or Contractual Requirement

The provision of personal data is partly required by law (e.g. tax regulations) or as a result of contractual provisions (e.g. information on the contractual partner). Sometimes it may be necessary to conclude a contract with personal data provided by you, which must subsequently be processed by us. You are, for example, obliged to provide Clancy with personal data when Clancy signs a contract with your organisation. The non-provision of personal data may have the consequence that the contract with you cannot be completed.

Purpose Of Clancy Websites

We adopt the above policy because we assume that visitors to our sites have a professional interest in the products and services we offer.

Use Of Clancy Group PLC's Website By Minors

Our site is intended for professionals working in, supplying to, or serving the process manufacturing industries, and thus not for minors under the age of 18. That said, you should not find anything on our site offensive or disturbing to minors - in fact minors may find much of the site's content educationally informative. We advise minors to seek parental approval before providing personal information or before visiting Clancy websites.

Review And Maintenance

If this Privacy Policy is amended or updated in any way, Clancy will place an updated version on this page. By regularly viewing this page you will ensure that you are always aware of what personal data Clancy collects and processes and under what circumstances, if any, we share personal data.

The DPO or nominated person will review this Policy at least annually.

Clancy will continue to review (audit) the effectiveness of this Policy to ensure it is achieving its stated objectives.



Safe. Successful. Sustainable. Secure. Skilled. Systems.