
Privacy Notice

September 2023

Version No	Date Issued	Update Details	Owner	Approved by	Policy Number
v4.0	February 2022	Notice in previous format	HR Director	The Board	POL-017
v5.0	September 2023	Notice finalised following revision and review of February 2022 Notice, amendments including how and when personal data is processed and change of format.	HR Director	The Board	POL-017

Privacy Notice

The Clancy Group Limited and its associated companies Clancy Plant Limited and Clancy Docwra Limited (Clancy or 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 Notice ("Notice") will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from), or if images of you are gathered on the CCTV and vehicle dashcam systems we use and tell you about your privacy rights and how the law protects you.

Notice

This Notice aims to give you information on how we collect and process your personal data through your use of this website, including any data you may provide through this website and also includes images of members of the public gathered on our CCTV and vehicle dashcam systems.

Other forms of processing described on this Notice which might include your personal data are:

- Our internal investigations (comprising driver collision investigations, data protection-related investigations and other investigations such as health, safety and environmental investigations);
- The use by our operational teams of information of residents at whose properties we are working;
- Use of our Learning Management System (LMS)
- Use by individuals (such as visitors and those making deliveries) of the sensor-operated automatic car park barrier at our Copper Mill Lane headquarters;
- Handling enquiries or complaints we receive from members of the public; and
- The Clancy Praise scheme.

It is important that you read this Notice together with any other privacy policies or fair processing policies we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This Notice supplements other notices and privacy policies and is not intended to override them.

This Notice does not apply to our employees, contractors, workers or candidates for employment or engagement (for whom we have separate internal privacy notices).

Controller: This Notice is issued on behalf of the Clancy Group so when we mention "Clancy", "we", "us" or "our" in this Notice, we are referring to the relevant company in the Clancy Group responsible for processing your data. The Clancy Group Limited is the controller and responsible for this website.

If you have any questions about this Notice, including any requests to exercise your legal rights, please contact our GDPR & DPA Compliance Officer using the details set out below.

Third Party Links

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy Notice of every website you visit.

The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which may include, but is not limited to:

- identity data including first name, unmarried name, last name, username or similar identifier, marital status, title, date of birth and gender;
- contact data including physical address if provided, email address and telephone numbers;
- geographic location;
- the date and time of access to the website;
- usage Data including information about how you use our website and services;
- CCTV footage and access control data (if attending our premises)(including gathering CCTV images from intruder movement-activated cameras;
- video images, taken by forward-facing dashcams mounted on our commercial vehicles and company cars of individuals and other traffic on public roads and pavements, our building sites and other properties (public and private) that our vehicles visit;
- residents' information (e.g. house number) where Clancy is carrying out works;
- facts and circumstances of investigations, enquiries, complaints and praise for Clancy staff;
- your vehicle's registration number (for our ANPR-operated car park barrier);
- technical data including internet protocol (IP) address, the Internet service provider of the accessing device, browser type and version, referral source and pages visited, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website; 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.

In some of the processing described on this Notice we may collect special categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). We may also, very rarely, collect information about criminal convictions and offences (e.g. in relation to internal investigations we carry out).

How is your personal data collected?

You may share your personal data with us for a variety of reasons.

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your identity and contact data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- apply for our products or services;
- subscribe to our service or publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey;
- give us feedback or contact us;
- interact with our website, we will automatically collect technical data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies.

We also receive personal information directly from you for one or more of the following reasons:

- when you communicate with us as an individual to exercise your rights;
- when you communicate with us in the context of an employee or worker representing an organisation that has procured Clancy services;
- when you communicate with us directly as an individual or as a customer of an organisation that has procured Clancy services;
- as a consequence of your usage of any of Clancy online services or mobile applications; and
- when video images are recorded by our CCTV equipment located in vehicles and buildings that are owned or operated by Clancy for the purposes of defending the safety and security of Clancy staff and members of the public, and Clancy properties and vehicles
- if you report or are involved in (e.g. as a witness) an incident which we investigate;
- if you have provided us with your vehicle's registration number to allow you to use our automatic ANPR-operated car park barrier;
- if you have submitted an enquiry or complaint to us; or
- you have complimented a member or members of our staff, such that we include your positive comments in our staff Praise scheme.

We also sometimes receive data about you (your contact information and any relevant vulnerabilities, such as deafness) from our clients, of whom you are a customer, when we are working at or near your property.

Contacting Clancy

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.

We use the information that has been given us to:

- deliver the content of our website correctly;
- respond to communications from you relating to services we provide to an organisation you represent, directly to you as an individual or as a customer of an organisation;
- examine and identify website and mobile application usage patterns to enable Clancy to improve our services;
- optimise the content of our website as well as its advertisement;
- protect the long-term viability of our information technology systems and website technology;

- detect and prevent criminal activity and assist in claim management;
- manage training activity records on our Learning Management System;
- investigate Health, Safety and Environmental incidents for example utility damage or personal injury claims;
- comply with Health and Safety legal compliance (for example, maintaining an accident book);
- to manage the contact information of residents at sites where Clancy is carrying out works;
- investigate data protection related internal investigations and investigations of alleged non-compliance with data protection legislation;
- facilitate Clancy's compliance with data subject rights requests and other compliance duties for example Data Subject Access Requests, personal data erasure requests, personal data rectification requests etc;
- manage internal investigations (in relation to the following types of investigations: alleged fraud by Clancy staff members, alleged H&S breaches, whistleblowing claims, internal disciplinary matters);
- Investigate drivers' post-incident (e.g., collision) or complaint investigations to gather details to determine escalation outcome);
- investigate and resolve enquiries and complaints;
- prevent and detect crime;
- allow entry into the Clancy Head Office (by virtue of the ANPR sensor-operated car park barrier); and
- provide to staff compliments and praise that were made by members of the public.

We analyse collected data and information statistically and, in the aggregate, with the aim of increasing the data protection and data security of Clancy and to ensure an optimal level of protection for the personal data we process.

How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- internally with Clancy employees and sub-contractors;
- where we need to comply with a legal obligation;
- where we need to perform the contract we are about to enter into or have entered into with you; and
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

Who we share your personal data with externally

We only share your personal data with third parties outside Clancy where we have a lawful basis for doing so. The recipient third parties are:

- our clients such as water and other utility companies;
- suppliers who provide services on behalf of Clancy, including Safer Scotland Ltd, Aptumo, Oneserve, Sphera, Learning Pool Ltd, Depotnet Ltd and Hikvision UK and Ireland Ltd;
- other third parties who perform services on our behalf, including insurers and professional advisors to Clancy;
- public bodies and regulatory authorities such as the Health & Safety Executive (including police and law enforcement agencies);

- providers of our IT and system administrative services; and
- any representative whom you have authorised to act on your behalf.

Our lawful basis for processing personal information

The lawful basis that we rely on for processing your personal data will vary depending on the context of how the information was collected or provided to us and the purpose for which the information was provided:

Our lawful bases for processing your personal data are:

- (a) where the use of our or third-party systems required your consent prior to the collection and processing of your information our lawful basis is your consent. This may arise for example, when you are completing online forms. You are able to withdraw your consent at any time and you can do this by contacting the Head of Internal Investigations (GDPR & DPA Compliance Officer) at Roland.Thomas@theclancygroup.co.uk
- (b) where we have a contractual obligation;
- (c) where we have legitimate interests except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data;
- (d) where we are subject to a legal obligation by which processing of personal data is required;
- (e) to protect your vital interests or that 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.

Where we process any of your special category personal data, or criminal data, Clancy needs another lawful reason to do so, in addition to the ones listed above. The conditions for processing such data we rely on are:

- (a) you have given you explicit consent to such processing;
- (b) it is necessary for the purposes of employment, social security or social protection law; or
- (c) you have made the data manifestly public yourself.

We will always seek your consent prior to using your data for any purpose that is not covered by another lawful basis.

How we store your personal information?

We maintain operational, technical and physical safeguards designed to protect personal information against accidental, unlawful or unauthorised destruction, loss, alteration, access, disclosure or use. We will store your personal data securely in a number of locations, including on Clancy sites and IT systems (including email and servers). The data of the server log files are stored separately from any personal data provided by users.

How long we retain personal information for

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.

CCTV recordings made at Clancy premises are retained for 90 days. The video files are deleted from all systems. Video images from vehicle-mounted dashcams are overwritten after 64 hours of driving footage is recorded.



Personal information contained in communications you make with us as an individual are retained for 90 days from the date of receipt unless such information is the subject of a claim or any legal action. Clancy will then retain such information for up to 90 days post completion of the claim or legal action. Following this, such information will be deleted from our systems and all paper copies securely shredded.

Personal information contained in communications you make with us while acting on behalf of an organisation will be retained for 7 years from the date of contract termination. Following this, such information will be deleted from our systems and all paper copies securely shredded.

Website and application usage information will be retained for 30 days. Thereafter such information will be anonymised in a manner so that it is not possible to reverse the anonymization method or link with any other data to derive an individual's identity.

We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- If you want us to establish the data's accuracy;
- where our use of the data is unlawful but you do not want us to erase it;
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; and/or
- you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your

consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request the transfer of your personal data to you or to a third party (data portability). We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

If you wish to exercise any of the rights set out above, please contact the Head of Internal Investigations (GDPR & DPA Compliance Officer) at Roland.Thomas@theclancygroup.co.uk

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

If you wish to exercise your rights and it relates to personal information you provided to another organisation that contracted with Clancy for Clancy to provide services to you then you must exercise your rights directly with that organisation.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Changes to the privacy Notice and your duty to inform us of changes

We reserve the right to update this Notice at any time, and we will provide you with a new Notice when we make any updates. If we would like to use your previously collected personal data for different purposes than those we notified you about at the time of collection, we will provide you with notice and, where required by law, seek your consent before using your personal data for a new or unrelated purpose. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

We keep this Notice under regular review. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.



Contact Details

If you have any questions about this Notice or how we handle your personal data, or would like to request access to your personal data please contact:

Roland Thomas at: roland.thomas@theclancygroup.co.uk

If you are unsatisfied with our response to any issues that you raise with us, you have the right at any time to make a complaint to the Information Commissioner's Office:

Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline number: 0303 123 1113

International transfers of personal information

We do not transfer data to countries outside of European Economic Area (EEA).