Supplementary Privacy Notice OneAdvanced (Fingerprint and facial recognition processing for time and attendance records purposes)

October 2024

Version No	Date Issued	Update Details	Owner	Approved By	Policy Number
v1.0	August 2023	First draft	Operations Director (Energy)	The Board	POL-017a
v1.1	July 2024	Policy finalised following revision and review of draft, with amendments.	Operations Director (Energy)	The Board	POL-017a
v1.2	Oct 2024	Addition of references to OneAdvanced and facial recognition processing	Operations Director (Energy)	The Board	POL-017a

Supplementary Privacy Notice (Fingerprint and facial recognition processing for attendance records purposes)

The Clancy Group Limited (Clancy, we, or us) is committed to protecting the privacy and security of your personal data. This Privacy Notice ("Notice") describes how we collect and process personally identifiable information (personal data) about you in regard to our use of fingerprint, facial and other personal data for recording the attendance of employees and sub-contractors on sites and to ensure that all of our data protection obligations are met in respect of this processing. What the UK GDPR calls 'biometric data' includes data generated by measurements of your biological characteristics, such as your fingerprint or facial features.

"Fingerprint and Facial Sign-in Data" collected by us in this process includes:

- your name;
- your enrolment date on to the fingerprint recording system;
- your job title;
- your shift pattern;
- log-in times and log out times on sites;
- the geographic location of any OneAdvanced terminal which you use;
- scans of your fingerprints (biometric data);
- scans of your face; and
- (if you are a direct employee) the last 4 digits of your employee number, or (if you are a sub-contractor) your assigned 4-digit Unique Identifier (UI).

Privacy Notice

This Notice describes the categories of personal data that we collect, how we use your personal data, how we secure your personal data, when we may disclose your personal data to third parties, and when we may transfer your personal data outside of your home jurisdiction. This Notice also describes your rights regarding the personal data that we hold about you, including how you can access, correct, and request erasure of your personal data. We will only process your personal data in accordance with this Notice unless otherwise required by applicable law. We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes.

It is important that you read this Notice together with any other privacy notice or fair processing policy 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 is reviewed annually by our Data Protection and Compliance Officer ("DPCO") or nominated person and will be monitored for compliance by the DPCO, and line managers/supervisors within their own area of responsibility. Routine audits will be carried out annually and may also include random and scheduled inspections by the DPCO. 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 your manager or the DPCO.

This Notice does not form part of any contract of employment, and we may amend it at any time.

Who does this Notice apply to?

This Notice applies to all staff working for Clancy on contracts for which we process your Fingerprint and Facial Sign-in Data to assist us to evidence your compliance with health and safety and other legal requirements, and for the purposes of the contract Clancy has with its client.

What Information do we collect?

This Notice explains how we process your Fingerprint and Facial Sign-in Data. We will never collect any unnecessary Fingerprint and Facial Sign-in Data from you and do not process your Fingerprint and Facial Sign-in Data other than as specified in this Notice.

Personal data is retained in restricted-access folders on the Clancy network and by the third-party processor company which supplies the Fingerprint and Facial Sign-in Data system, OneAdvanced.

We take your privacy very seriously and will never sell your data.

Use of personal data including our lawful bases for processing personal information

We only process your personal data where applicable law permits it for recording the attendance of employees and sub-contractors on sites, to ensure that all of our data protection obligations are met in respect of this processing.

We process your Fingerprint and Facial Sign-in Data for the following legitimate business purposes:

- to manage the attendance of employees and sub-contractors on sites and to verify your weekly payroll; and
- to identify the location of employees and sub-contractors using a fixed geographic location, where this is required, under our contract with a client.

OneAdvancedWe rely on your explicit consent as the lawful basis for processing of your Fingerprint and Facial Sign-in Data, which consent you may withdraw at any time without detriment to you. If you choose not to give your consent to this processing, you will be offered an alternative means of signing in to and signing out of sites by using your Clancy IAM card or fob. If you choose this alternative means, which does not use scans of your fingerprint or face to identify you and therefore does not involve the processing of your special category personal data (see the section below in this Notice 'Collection and Use of Special Categories of Personal Data'), the lawful basis for the processing of your data which we rely on will be that it is necessary for our legitimate interests.. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

Collection and Use of Special Categories of Personal Data

The following special categories of personal data are considered sensitive and may receive special protection:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;

- genetic data;
- biometric data (when used to identify a particular person);
- data concerning health; and
- data concerning sex life or sexual orientation.

Data relating to criminal convictions and offences also receive special protection.

We will only retain special categories of personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, or reporting obligations, or as necessary to resolve disputes.

Who has access to your personal data?

We will only disclose your personal data to third parties where required by law or to our employees, sub-contractors, designated agents, or third-party service providers who require such information to assist us with administering the Fingerprint and Facial Sign-in Data system, including the third-party service provider, OneAdvanced, who provide services to us or on our behalf.

We require OneAdvanced to implement appropriate security measures to protect your personal data consistent with our policies and any data security obligations applicable to us as your employer. We do not permit OneAdvanced to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes in accordance with our instructions.

When we disclose your personal data to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal data necessary for the specific purpose and circumstances.

Data security

We take data protection seriously, and as such, we have internal policies/procedures (such as our Data Protection Policy, Data Breach and Incident Management Policy, and Records Management Policy). We also maintain a range of security controls in place to ensure that your personal data is not lost, accidently destroyed, misused or disclosed, and is not accessed except by Clancy staff in the performance of their duties, or third-party personnel in performance of the contract we have with their employers.

We have implemented appropriate physical, technical, and organizational security measures designed to secure your personal data against accidental loss and unauthorized access, use, alteration, or disclosure. In addition, we limit access to personal data to those employees, agents, sub-contractors, and other third parties that have a legitimate business need for such access.

We do not transfer or store any Fingerprint and Facial Sign-in Data outside the UK.

Fingerprint and Facial Sign-in Data retention

Fingerprint and Facial Sign-in Data is retained by the processor OneAdvanced for the term of Clancy's contract with it, and after termination of the contract will be returned by OneAdvanced.

Under some circumstances we may anonymize your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. Once you are no longer a staff member of the company, we will retain and securely destroy your personal data in accordance with our Records Management Policy and applicable laws and regulations.

Details of retention periods for different aspects of your personal data are available in our Records Management Policy which can be found on One Clancy, or alternatively, requested from the HR Department.

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 (DPCO) 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 request specific information from you to help us confirm your identity and 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.

Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

More information can be found on the processing of your personal data in Clancy's Individual Rights Policy.

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 this 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. Historic versions can be obtained by contacting us. 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