CUNDALL

POLICY

Data Protection

Job No: HR Policy
Doc Ref: HR/042
Latest Revision: F
Date: 14/02/2018

Project Name:	**HR Policy and Procedure**
Client:	Cundall
Report Title:	Data Protection Policy
Job Number:	N/A

Document Revision History

Revision Ref	Issue Date	Purpose of issue / description of revision
D	14/02/2017	Updates to policy to reflect changes in UK legislation
E	14/02/2018	Comprehensive review to comply with UK GDPR
F	15/02/2018	IT Amended Security Information
H	28/02/2018	Further updates to reflect changes in UK legislation

Document Validation (latest issue)

X	X	X
Principal author Carole O'Neil	Checked by Graeme Padgham	Verified by Tomas Neeson

1. General Principles

1.1 Scope

Cundall is committed to being transparent about how it collects and uses the personal data of its workforce (and others), and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns and apprentices, and former employees, (HR-related personal data). It also includes a section on the processing of clients' personal data.

We have appointed Graeme Padgham, IT Director, as the person with responsibility for data protection compliance within the organisation. He can be contacted at g.padgham@cundall.com. Questions about this policy or requests for further information should be directed to him.

1.2 Definitions

"Personal data" is any information that relates to an individual who can be identified from that information.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and biometric data.

1.3 "Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings. Data Protection Principles

Cundall processes HR-related personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate records of personal data, and take reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing, in our privacy notices. We will not process personal data of individuals for other reasons.

In relation to any processing activity we carry out, we will review the purpose of that particular activity and select the most appropriate lawful basis for that processing i.e.:

- that the individual has consented to the processing;
- that the processing is necessary for the performance of a contract to which the individual is a party or in order to take steps prior to entering into a contract;
- that the processing is necessary for compliance with a legal obligation to which we must comply with;
- that the processing is necessary for the protection of the vital interests of the individual or another person;
- that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
- that the processing is necessary for the purposes of our legitimate interests.

Where we process special categories of personal data or criminal records data to perform obligations or exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

We will update HR-related personal data promptly if an individual advises that their information his/her information has changed or is inaccurate.

Personal data gathered during the employment / worker / contractor or volunteer relationship, or during the apprenticeship / internship is held in the individual's personal file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

We keep a record or our processing activities in respect of HR-related person data in accordance with the requirements of the General Data Protection Regulations (GDPR).

1.4 Policy Review

We will review and update this policy regularly in accordance with our data protection obligations.

2. Staff Data

2.1 Individual Rights (Staff Data)

As data subjects, individuals have a number of rights in relation to their personal data.

2.1.1 Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, we will tell him/her:

- whether or not his/her data is processed (and if so, why), the categories of personal data concerned, and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA), and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks we have failed to comply with his/her data protection rights; and
- whether or not we carry out automated decision-making, and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to hradministrator@cundall.com. In some cases, we may need to ask for proof of identification before the request can be processes. We will inform the individual if we need to verify his/her identity, and the documents required.

We will normally respond to a request within a period of one month from the date it is received. In some cases (such as where we process large amounts of the individual's data) we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we may agree to respond, but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If an individual submits a request that is unfounded or excessive, we will notify him/her that this is the case, and whether or not we will respond to it.

2.1.2 Other Rights

Individuals have a number of other rights in relation to their personal data. They can require Cundall to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;

- stop processing or erase data if the individual's interests override Cundall's legitimate grounds for processing date (where we rely on our legitimate interests as a reason for processing the data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override Cundall's legitimate grounds for processing data.

To ask us to take any of these steps, the individual should sent the request to hradministrator@cundall.com.

3. Data Security (Staff Data)

We take the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed except by employees in the proper performance of their duties. These include:

- Password protection on IT systems storing HR-related personal data;
- Hard copy data is securely stored, and accessible only to staff who have a legitimate need to access the data for the proper performance of their duties;
- A "clear desk" policy within the Human Resources team;
- Restrictions on the removal of personal data from our premises, without appropriate safeguards;
- The use of encryption technology when communicating personal data electronically; Bitlocker Encryption on all USB devices holding sensitive data, email encryption used for sensitive communications.
- Windows Active Directory Security groups restrict access to sensitive data.

3.1 International Data Transfers

HR-related personal data may be transferred to countries outside the EEA to support project-related activities in other territories, manage staff mobility and international transfers, and/or otherwise facilitate the administration of an international business. Data is transferred outside the EEA only where necessary for the purposes outlined above, and in line with the principles of this policy.

3.2 Individual Responsibilities

Individuals are responsible for helping us keep their personal data up to date. Individuals should let us know if data provided to us changes, for instance if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, we rely on individuals to help us meet our data protection obligations to staff and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access, and only for authorised purposes;
- not to disclose data except to individuals (whether within or outside Cundall) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access (including password protection) and secure file storage and destruction);
- not to remove personal data (or devices containing or that can be used to access personal data) from our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about our security procedures can be found in our IT Security policy.

We take compliance with this policy very seriously. Failure to comply with the policy puts at risk the individuals whose personal information is being processed, and carries the possibility of significant civil and criminal sanctions for the individual who caused the issue and for us and may in some circumstances amount to a criminal offence by the relevant individual.

Failure to comply with these requirements may amount to a disciplinary offence, which will be dealt with under our disciplinary procedures. Significant or deliberate breaches of this policy (such as accessing employee or customer data without authorisation or a legitimate reason to do so, or deliberately or carelessly compromising the security of such data) may constitute gross misconduct and may lead to dismissal without notice.

3.3 Training

We provide training to all individuals about their data protection responsibilities as part of our induction process.

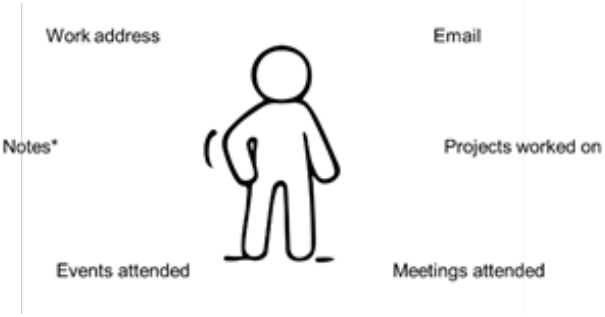
Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their responsibilities and how to comply with them.

4. Client Data

4.1 Scope

This section of the policy applies to our global business.

4.2 Data map



*can include project notes, feedback comments, preferences but no special information.

4.3 Lawful Basis

We hold limited data under the GDPR lawful basis of "legitimate interest". This is to enable us to work as a trusted advisor to our clients and contacts in the industry. We take this extremely seriously to ensure that this is transparent, fair, necessary and limited.

In order to fulfil these important requirements, we carry out a legitimate interests assessment. As part of this assessment, we conduct a balancing test to establish whether or not our interests affect or interfere with the individual's freedoms and rights.

Our uses of personal data include:

- inviting people to thought leadership events or industry events;
- updating individuals in the industry on relevant legal or regulatory changes;
- informing individuals about a project that they might be interested; and
- giving people updates on Cundall services, locations or other progress.

As an organisation we have an obligation to work with our clients, contacts, and the wider industry to share our ideas and thought leadership and help to raise standards. We do this by focusing on four areas, our "Four Cornerstones".

These are

- Our Projects
- Our Offices
- Our Homes and Communities
- Industry Leadership.

To enable us to do this we contact our clients and contacts when we feel there is information that is in their interest.

4.4 External parties

We will never share personal information with externally controlled parties. Processors are vetted to ensure that they comply with GDPR and data protection requirements. We may transfer personal data outside of the European Economic Area (EEA) to one of our numerous offices around the world that are all associated with the Limited Liability Partnership. Cundall Johnston & Partners LLP has put in place agreements with its overseas entities which reflect the European Commission's model contractual clauses governing the transfer of personal data from the Community to third countries. Client information is not shared outside this Group.

4.5 Right to correct or access

Individuals included in our database have the right to correct or access their information at any time. To do so, clients should contact their main Cundall contact or globalmarketing@cundall.com.

4.6 Portability

We can issue an individual's data to them in a portable form as requested by them.

4.7 Right to erasure

Individuals have the right to object to their information being used for the purposes listed above and can request that they are removed from our database at any time unless there is a legal reason for us to keep information on record.

4.8 Records

We will keep written records of all of our processing activities relating to client data as required under the GDPR regulations.

All personal data will be kept securely in accordance with out information security policy. We will retain personal data for the purposes listed above until we decide the services we provide are no longer relevant to the individual or in rare cases indefinitely where necessary for business efficacy.

4.9 The right to lodge a complaint

Individuals can contact Graeme Padgham at g.padgham@cundall.com in the event that:

- they are concerned or suspect that personal data processing without a lawful basis is taking place;
- a data breach has occurred;
- personal information has been accessed without the proper authorisation;
- personal information has not kept or deleted securely;
- personal information has been removed from our premises without appropriate security measures being in place;
- a breach of this policy has occurred; or
- there has been a breach of any of the data protection principles set out in paragraph 1.3.

5. Data breaches

5.1 Scope

A data breach can be:

- the loss or theft of data equipment on which personal information is stored;
- unauthorised access to personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems failure;
- human error such as an accidental deletion of alteration of data;
- unforeseen circumstances such as a fire or flood;
- a deliberate attack on Cundall's IT systems, such as hacking, viruses or phishing scams; or
- blagging offences where information is obtained by deceiving the organisation which holds it.

5.2 Action we will take

In the event of any of the above data breaches, we will aim within 72 hours of becoming aware of the issue to report the breach to the Information Commissioner's Office if we think it will affect the rights and freedoms of any individuals. We will also notify any affected individuals in the event of such a data breach.

www.cundall.com

Asia Australia Europe MENA UK & Ireland