Data Protection Policy

Introduction

Nviro is committed to being transparent about how it collects and uses the personal data of its workforce and meeting its data protection obligations.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

Nviro has appointed Marc Goodey, Deputy Managing Director and Finance Director, as the person with responsibility for data protection compliance within the Company. Questions about this policy, or requests for further information, should be directed to them. Marc can be contacted at communications@nviro.co.uk.

Policy Aim

This policy sets out Nviro's commitment to data protection and individual rights and obligations in relation to personal data.

The policy is compliant with the UK General Data Protection Regulation (UK GDPR).

This policy does not form part of the contract of employment, and we reserve the right to amend or withdraw it at any time.

Definitions

"Personal data" is any information that relates to a living 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.

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

Data Protection Principles

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

1. personal data is processed lawfully, fairly and in a transparent manner;
2. personal data is collected only for specified, explicit and legitimate purposes;
3. personal data only processed where it is adequate, relevant and limited to what is necessary for the purposes of processing;
4. only accurate personal data is kept, and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay;
5. appropriate measures are adopted to make sure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage;
6. personal data is kept only for the period necessary for processing.

Nviro is transparent with the reasons for processing individual personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data for other reasons. If Nviro wants to start processing HR-related data for other reasons than stated in the privacy notice, individuals will be informed of this before any processing begins.

HR-related data will not be shared with third parties, except as set out in our privacy notices. Where Nviro relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where Nviro processes criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with the Company's Safeguarding policy.

Individuals should advise the Company of any changes to personal data by logging onto the employee portal and updating their information. This will help to ensure that only accurate data is held by the Company.

Personal data gathered during the employment is held in the individual's personnel file in electronic format and on HR and IT systems, as detailed in the Colleague Privacy Notice.

The periods for which the Company holds HR-related personal data are contained in its privacy notices.

Nviro keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the UK GDPR.

Individual Rights

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

Subject access requests

Individuals have the right to make a subject access request. When a request is received Nviro will provide the individual with a copy of the personal data undergoing processing or the specific data that has been requested. This will be in electronic format.

To make a subject access request, the individual should send the request to the HR Department at communications@nviro.co.uk. In some cases, Nviro may need to ask for proof of identification before the request can be processed.

Nviro will normally respond to a request within one month from the date it is received. In some cases, such as where the request is complex, it may be necessary to request an extension. Nviro will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, Nviro is not obliged to comply with it. Alternatively, Nviro can 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 if it is made with the intention of harassing the Company or causing disruption, or excessive where it repeats a request to which Nviro has already responded.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation 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 Nviro's legitimate grounds for processing 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 the individual's interests override Nviro's legitimate grounds for processing data.

To ask Nviro to take any of these steps, the individual should send the request to communications@nviro.co.uk

Data Security

All records of a personal and/or sensitive nature will be kept in a secure environment with access only allowed to those persons that require it to perform their job, or where a particular function has been requested by the senior management of the company. Wherever possible records are held electronically on the company's secure servers. Files stored electronically are held in folders where access is restricted via user logins.

Documents relating to the following should be kept for a period of six years:

- Customer records
- Financial records
- Payroll records
- Personnel records
- Contract documentation

After this period, electronic records are deleted from the company's servers. Paper records are shredded using internal shredders.

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 inside or outside the company) 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).
- to report data breaches to the HR Department immediately.

If the Company sells all or part of its business, or loses a cleaning contract to another Company, it may provide personal data about its employees to any prospective purchaser in the course of negotiations. So far as possible, such data will be provided in an anonymous format and if this is not possible the prospective employer will be required to keep the information confidential. The Company will transfer any personal data on any transfer or sale falling in a secure format and within the terms of the Transfer of Undertakings (Protection of Employment) Regulations 2006 ('TUPE').

Data Breaches

Failing to adhere to the requirements set out in this policy may result in an employee incurring personal criminal liability and amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

If Nviro discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Nviro will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

Nviro does not generally transfer data outside of the UK, however on occasions when an individual is absent from work or has left the business and staying/living abroad, it may be necessary to transfer data outside of the UK, this will be directly with the employee themselves or authorised persons.

Individual Responsibilities

Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the company know if the data provided changes, for example, if an individual moves house, changes names or bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment. Where this is the case, the company relies on individuals to help meet its data protection obligations to staff and to customers 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 inside or outside the company) 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 the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to [name of individual/the data protection officer] immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

Nviro will provide training to all individuals about their data protection responsibilities as part of the induction process and every year thereafter.