


| | | | |
|---|-------------------------|------------------------------|------------------------|
|  | Policy Documents | | |
| | DOCUMENT TITLE: | Data Privacy and GDPR Policy | Code: |
| | WRITTEN BY: | Steve Hughes - CNL | Issue Number :1 |
| | APPROVED BY: | Sarah Davies | |
| DATE OF CHANGE: | 21.05.18 | Page 2 of 7 | |

1 DATA PRIVACY AND PROTECTION STATEMENT

- 1.1 N-Virocycle has the highest regard for the security and protection of confidential information. Our business processes and systems are therefore designed with data privacy and data protection in mind.
- 1.2 N-Virocycle provides cost-effective recycling solutions for Industry and Agriculture. During the course of our business activities we will collect, use, store and process confidential information in order to carry out our business activities. We will only collect the data that we need for these purposes. In addition to our customers, we also hold data relating to our suppliers and for the people who work for us. We are fully committed to keeping that data secure.

2 ROLES & RESPONSIBILITIES


- 2.1 The individual with overall responsibility for information security and GDPR at N-Virocycle is the Operations Director.
- 2.2 The Compliance & Technical Manager is responsible for IT & data security on a day-to-day business.
- 2.3 All staff are responsible for data security, regardless of whether or not they use a computer to carry out their work. All data security issues should be reported, in the first instance to the compliance & technical Manager. If unavailable, for example due to holiday, then queries should be directed to the Operations & Contracts Manager or Business Manager.

3 GDPR TRAINING

All staff will receive Data Privacy and GDPR training so that they understand their responsibilities and all aspects of good and poor data protection practice.


4 GENERAL DATA PROTECTION REGULATIONS (GDPR)

- 4.1 GDPR is an EU Regulation that became law on 25 May 2018. GDPR replaced the UK's Data Protection Act 1998 (DPA) without the need for further UK legislation. Upon Brexit the legislation will stay in place.
- 4.2 GDPR is more demanding than the 1998 Data Protection Act. All organisations will be expected to obey the Act and there will be fines for those who transgress. Recent fines from the Information Commissioners Office (ICO) make clear that

| | | | |
|---|-------------------------|------------------------------|------------------------|
|  | Policy Documents | | |
| | DOCUMENT TITLE: | Data Privacy and GDPR Policy | Code: |
| | WRITTEN BY: | Steve Hughes - CNL | Issue Number :1 |
| | APPROVED BY: | Sarah Davies | |
| | DATE OF CHANGE: | 21.05.18 | Page 3 of 7 |

they will punish transgressors. This includes individuals and companies. Many of the recent transgressors are charities and small businesses.

- 4.3 The new maximum fines are 4% of annual global turnover or €20 million, whichever is higher, for failing to protect data or 2% of annual global turnover or €10 million, whichever is higher, for the failure of internal data protection processes.
- 4.4 The data protection principles, as set out in the UK's Data Protection Act 1998 (DPA), remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:
1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
 2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
 4. Accurate and, where necessary, kept up to date.
 5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
 6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 4.5 N-Virocycle is a data controller.
- 4.6 Like the Data Protection Act, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
- 4.7 GDPR refers to sensitive personal data as "special categories of personal data." For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

|  | Policy Documents | | |
|---|------------------------|------------------------------|-----------------|
| | DOCUMENT TITLE: | Data Privacy and GDPR Policy | Code: |
| | WRITTEN BY: | Steve Hughes - CNL | Issue Number :1 |
| | APPROVED BY: | Sarah Davies | |
| DATE OF CHANGE: | 21.05.18 | Page 4 of 7 | |


5 CONSENT

- 5.1 The GDPR requires data controllers to have a lawful basis for processing personal data. If they rely on the consent of the data subject, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being processed.
- 5.2 N-Virocycle processes two main types of personal data: business data and staff data. In addition N-Virocycle process personal data for people who use our website. The website privacy notice will make clear how this is used

| | Lawful basis for processing: |
|--|------------------------------|
| Business Data Contact data and banking data for customers and suppliers | Contract |
| Staff data Personal and potentially person-sensitive data, plus banking details | Contract |
| Website users IP address plus email details if request further information | Informed consent |

6 CHILDREN

- 6.1 According to the GDPR, children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerns and their rights in relation to the processing of personal data. Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- 6.2 N-Virocycle's policy with regard to children and GDPR is that it does not process personal data for children.

| | | | |
|---|-------------------------|------------------------------|------------------------|
|  | Policy Documents | | |
| | DOCUMENT TITLE: | Data Privacy and GDPR Policy | Code: |
| | WRITTEN BY: | Steve Hughes - CNL | Issue Number :1 |
| | APPROVED BY: | Sarah Davies | |
| | DATE OF CHANGE: | 21.05.18 | Page 5 of 7 |

7 INDIVIDUAL RIGHTS

7.1 Individuals have the following rights under GDPR:

1. The right to be informed

The right to be informed encompasses the obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how organisations use personal data.

The information supplied about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language,
- free of charge.

2. The right of access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data

Organisations can no longer charge a fee for providing information and must supply the information within 30 calendar days of the request.

3. The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If organisations have disclosed the personal data in question to third parties, they must inform them of the rectification where possible. They must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

4. The right to erasure


The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

5. The right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, organisations are permitted to store the personal data, but not further process it. Organisations can retain just enough information about the individual to ensure that the restriction is respected in future. An example would be to retain the minimum data to ensure continuing exclusion from mailshots and marketing campaigns.

6. The right to data portability

| | | | |
|---|-------------------------|------------------------------|------------------------|
|  | Policy Documents | | |
| | DOCUMENT TITLE: | Data Privacy and GDPR Policy | Code: |
| | WRITTEN BY: | Steve Hughes - CNL | Issue Number :1 |
| | APPROVED BY: | Sarah Davies | |
| DATE OF CHANGE: | 21.05.18 | Page 6 of 7 | |

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. The right to object

Individuals have the right to object to:

- i. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- ii. direct marketing (including profiling)
- iii. processing for purposes of scientific/historical research and statistics.

If an organisation processes personal data for direct marketing purposes:

- iv. It must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.
- v. It must deal with an objection to processing for direct marketing at any time and free of charge.
- vi. It must inform individuals of their right to object “at the point of first communication” and in its privacy notice.
- vii. This must be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.


8. Rights related to automated decision making and profiling

GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

8 SECURITY AND BREACH NOTIFICATION

- 8.1 Under GDPR legislation N-Virocycle has a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
- 8.2 A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows organisations to provide information in phases. If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay. Failing to notify a breach when required to do so can result in a significant fine, up to 10 million Euros or 2 per cent of global turnover.

N-Virocycle’s policy and procedure for responding to a data breach is outlined in the Data Breach Policy.

| | | | |
|---|-------------------------|------------------------------|-----------------|
|  | Policy Documents | | |
| | DOCUMENT TITLE: | Data Privacy and GDPR Policy | Code: |
| | WRITTEN BY: | Steve Hughes - CNL | Issue Number :1 |
| | APPROVED BY: | Sarah Davies | |
| DATE OF CHANGE: | 21.05.18 | Page 7 of 7 | |

9 WHERE IS DATA IS STORED AND PROCESSED?

- 9.1 The GDPR requires that data is only stored in countries where there is an adequate level of data protection, whether by the country's domestic legislation or of the international commitments it has entered into.
- 9.2 In most instances N-Virocycle stores digital data on its server at its office in Tewkesbury. Backup data may be stored in the Cloud (Internet). N-Virocycle will always seek to only store personal data in countries on the EU approved list.

10 GDPR DOCUMENTATION

The GDPR contains explicit provisions about documenting processing activities. N-Virocycle will therefore adhere to the following guidance taken from the Information Commissioner's website:¹

- N-Virocycle will maintain records as required on processing purposes, data sharing and retention.
- N-Virocycle may be required to make the records available to the ICO on request.
- Documentation can help N-Virocycle comply with other aspects of the GDPR and improve our data governance.
- N-Virocycle is a data processor and therefore has documentation obligations.
- As a smaller organisation, documentation requirements are limited to certain types of processing activities.
 - ¹ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/>

11 REVISION SUMMARY

11.1 First issue

John Edwards
Operations Director – N-Virocycle Ltd

Signed  Print Name: JEOWARDS Date approved: 25/5/18 Review Date: 24/5/19

Privacy Policy

1. Data Protection

We will only use the personal information (Personal Data) you provide to us to provide the Services, or to inform you about similar services which we provide, as long as you tell us in writing (via the opt in box on our contact form) that you want to receive this information. We will not pass your data to third parties save with your express authority.

1.1 In respect of your personal data we will

- (a) process that Personal Data only on your written instructions unless we are required by the laws of any member of the European Union or by the laws of the European Union applicable to us (Applicable Laws) to process Personal Data. Where we do so we shall promptly notify you of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit us from so notifying you;
- (b) ensure that we have in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;
- (c) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and
- (d) notify you without undue delay on becoming aware of a Personal Data breach;
- (e) on receipt of a written request by you, delete or return Personal Data and copies on termination of the agreement unless required by Applicable Law to store the Personal Data; and if no such request is made we will ensure that the data is kept and maintained in a secure location.
- (f) maintain complete and accurate records and information to demonstrate compliance with this clause.

John Edwards
Operations Director – N-Virocycle Ltd

Signed  Print Name JEEDWARDS Date approved 25/5/18 Review Date 24/5/19

