GDPR POLICY STATEMENT

Version 3 revised 27/04/2021

NOVATI

AT THE CENTRE OF INNOVATION

Revision History

Revision	Date	Author	Description
1	24/05/2018	Philip Martin	GDPR policy statement
2	28/01/2020	Philip Martin	3.1.2 clause clarified and reference to May 2018 login removed.
3	27/04/2021	Matt Batey	Updated to reflect Novati branding

Approval History

Revision	Date	Approved by
1	25/05/2018	Les Clayton (SHEQ Director) & Matt Batey (IM&T Director)
2	28/01/2020	Matt Batey (IM&T Director)
3	27/04/2021	Matt Batey (IM&T Director)

GDPR Policy Statement

Introduction

The General Data Protection Regulations (GDPR) otherwise known as *the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* becomes enforceable from the 25th May 2018 and provides EU citizens with greater control over their personal data and the companies which hold it.

This policy document sets out our, UK Waste Solutions Limited's (Novati), obligations and procedures regarding the collection, processing, storage and disposal of personal data. We feel GDPR is a positive development, redressing the balance of power between customers and companies, and making us strive to be better. Here are a few key terms that you may have heard about in relation to GDPR:

Data Subject this refers to you, our customer.

Personally identifiable information (PII) is any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person. Such information can include medical, educational, financial, legal and employment records. Some forms of PII, which may not be apparent, are online identifiers such as an IP address, email address, biometric data and social media 'aliases'. Information such as an online identifier – e.g. an IP address – can be classified as personal data.

Personal Data this collectively refers to the PII that we hold on you.

1 The Rights of Data Subjects

GDPR provides you with the following rights, please refer the relevant parts of this policy for further details:

1.1 The right to be informed (Part 10)
1.2 The right of access (Part 11)
1.3 The right to rectification (Part 12)
1.4 The right to erasure (Part 13)
1.5 The right to restrict processing (Part 14)
1.6 The right to data portability (Part 15)
1.7 The right to object (Part 16)
1.8 To exercise any of these rights please either;
1.8.1 Call our Customer Services team on 01636 640744;
1.8.2 Email us at privacy@novati.co.uk

2 Lawful, Fair and Transparent Data Processing

2.1 We hold information about our customers, which is relevant to providing you with the best service possible. For example, we store your name, email address and telephone number to contact you in respect of these services.

2.2 As our customer, we have a legitimate interest in retaining and using this information to provide the contracted services. We promise to keep this information secure by using the best technological solutions available including encryption, multi-factor authentication and purpose-built systems.

2.3 We promise not to sell your personal data and restrict our data processing to meet the commitments to customers in the provision of services and any legal requirements incumbent upon us.

3 Specified, Explicit and Legitimate Purpose

When we run marketing campaigns, promotions and similar events, we promise not to contact you unless you have explicitly expressed your interest (known as consent) or are considered a legitimate interest.

3.1 To review or amend your consent preferences, please either log into the Hub or contact our Customer Service department on 01636 640744.

3.1.1 Please note an account is required to access the Hub.

3.1.2 Hub users are required to specify their consent preferences upon their first login and can subsequently change these preferences at their discretion.

3.2 Consent is considered valid for 24 months from the last date of the last amendment.

3.3 Legitimate interest, where the following tests are satisfied.

3.3.1 Where a clear benefit to the business is demonstrable

3.3.2 Where a potential benefit to the end customer is identifiable

3.3.3 It is considered that no harm or distress will result from the communication

3.3.4 Participation in, and response to previous campaigns is considered

3.3.5 The customer is not opted out of the communication type

4 Adequate and Limited Data Processing

4.1 We promise to only use your personal data in relation to services we provide you, within the bounds of legitimate interest, and for those purposes you opted into, please see item 3.

5 Accuracy of Data and Keeping Data Current

5.1 We work hard to ensure that the data we hold is accurate and we will contact you to ensure this remains true, however if you are aware of any inaccuracies please do let us know and we will be happy to make an amendment.

5.2 Please note that 5.1 is in addition to your right to rectification.

6 Data Retention

6.1 We will not keep your data for any longer than is necessary in respect of the purposes it was originally collected, held and processed for.

6.2 We will retain data in compliance with applicable laws and regulations.

6.3 For full details of our retention policies please refer to our Data Retention Policy.

7 Secure Processing

7.1 We will ensure that any processing of your data is performed securely and is protected against unauthorised access, unlawful processing and against accidental loss, destruction or damage.

7.2 If we employ a third party to assist in processing your data, we shall ensure they comply with all GDPR and this Policy.

8 Accountability and Audit

8.1 Our Data Protection Officer is Philip Martin, he may be contacted at privacy@novati.co.uk

8.2 We will keep internal records of all personal data collection, holding and processing, which shall incorporate the following information:

8.2.1 The name and details of the Company, its Data Protection Officer and any applicable third-party data processors.

8.2.2 The purposes for which the Company collects, holds and processes personal data;

8.2.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

8.2.4 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

8.2.5 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

9 Data Protection Impact Assessments

9.1 We will carry out Data Protection Impact Assessments for all new projects and/or new uses of personal data which involve the use of new technologies or where processing is likely to result in a high risk to rights and freedoms under GDPR.

9.2 Data Protection Impact Assessments will be overseen by the Data Protection Officer and shall address the following:

9.2.1 The type of personal data that will be collected, held and processed;

9.2.2 The purpose(s) for which personal data is to be used;

9.2.3 A change in the parties who are involved in the process;

9.2.4 Risks posed to data subjects; and

9.2.5 Proposed measures to minimise and mitigate identified risks.

10 Right to be informed

10.1 We will keep you informed of any changes about how we collect or use personal data.

10.2 We will keep you informed of any changes to our privacy policy.

10.3 We will regularly review our privacy policy and update it where necessary.

11 Right of subject access

You have the right to request a copy of the personal data that we hold on you, this is known as a subject access request.

11.1 To make a subject access request please contact us using one of the contact methods listed in 1.8 and request a copy of the data that we hold on you.

11.2 We will provide the information within 30 days unless there are exceptional circumstances, in either event we will keep you informed.

11.2.1 If the DPO determines there are exceptional circumstances the information delivery window will be extended to 90 days.

11.3 This service is free unless the request is deemed to be manifestly unfounded, excessive or repetitive in which case we will inform you of the administrative fee.

11.3.1 The determination of manifestly unfounded, excessive or repetitive subject access requests shall be made by the Data Protection Officer.

12 Right to rectification

You have the right to rectify inaccurate information that we hold.

12.1 To rectify information please contact us using one of the contact methods listed in 1.8 and provide details of the information to be corrected.

12.2 Where the supplied correction is questionable we shall seek further information to clarify the position.

13 Right to erasure (right to be forgotten)

You have the right to request the personal data that we hold on you is removed and deleted.

13.1 To exercise your right to erasure please contact us using one of the contact methods listed in 1.8 and request the erasure of your personal data.

13.2 We will comply with your request unless we are legally obliged to retain the personal data for a specified period, for example if you have placed an order or signed a contract. In these circumstances we will inform you of the legal constraint. For further information, please see our Data Retention Policy.

13.3 We will retain a nominal record of your personal data that is sufficient to identify you and the subsequent request to remove your data from our systems for audit purposes.

14 Right to restrict processing

You have the right to request that we suspend the processing of your data.

14.1 To exercise your right to restrict processing please contact us using one of the contact methods listed in 1.8 and provide details of the desired restriction(s).

15 Right to data portability

You have the right to request a copy of the personal data in our system.

15.1 To exercise the right to data portability please contact us using one of the contact methods listed in 1.8 and request a copy of your portable data.

15.2 We will provide this information in comma separated variable (CSV) format.

15.3 Requests will be completed within 30 days.

15.4 There is no charge for this service.

16 Right to object

You have the right to limit how we use your data. Please refer to Part 3 for how we use your personal data.

16.1 To exercise your right to object please contact us using one of the contact methods listed in 1.8 and provide details of the objection.

17 Personal Data Collected, Held and Processed

We may collect, hold and process the following personal data. For details of the data retention, please refer to our Data Retention Policy.

Type of Data	Purpose of Data
Forename / Surname	To address our customers
Job title	To address our customers
Email address	To enable us to contact our customers by email
Postal address	To enable us to contact our customers by post
Landline / Mobile phone number	To contact our customers by telephone
Bank account number / sort code	To arrange direct debit payments when requested
Credit / Debit card details	To take payment as instructed
Special categories: Disability and Dietary requirements	For the purpose of being considerate when arranging meetings, functions and similar events

18 Data Security – Storage

We take data security seriously and promise to follow the measures below:

18.1 All electronic copies of data shall be protected using secure passwords.

18.2 Sensitive personally identifiable data and critical resources shall be protected with secure passwords and multi-factor authentication. Where such information is transmitted it shall be encrypted.

18.3 Employee, sub-contractor and third-party access to data will be provisioned using the principle of least privilege[1].

18.4 Personal data shall only be held on company hardware or where appropriate with approved and verified third-parties. Transferring data to personal devices is strictly prohibited.

19 Data Security – Disposal

When disposing of personal data, we promise to do so securely by following these procedures:

19.1 Contact details will be removed from the Hub.

19.2 Data stored on file servers shall be securely deleted.

19.3 Where hardware is retired from the business we will securely delete all data storage using Microsoft's Secure Delete (SDelete) application which implements the Department of Defense clearing and sanitizing standard DOD 5220.22-M.

19.4 Personal data in hardcopy format shall be securely destroyed on-site using appropriate shredders.

19.5 Where third-parties hold data on our behalf we will ensure that data disposal mechanisms are GDPR compliant.

20 Data Security – Use of Personal Data

We promise to ensure that the following measures are taken with respect to the use of personal data:

[1] The Principle of least privilege promotes assigning the minimum permissions required to a user for them to perform their job successfully. This reduces the attack surface and exposure to restricted material within the business.

20.1 No personal data will be shared informally and if an employee, sub-contractor or third-party requires such information a formal request shall be submitted to the HR Director (hr@novati.co.uk).

20.2 No personal data will be transferred to an employee, sub-contractor or third-party without authorisation from the HR Director (hr@novati.co.uk).

20.3 Personal data will be handled with care and will not be left unattended or on view to authorised employees, sub-contractors or third-parties.

20.4 If personal data is viewed on a computer and the user leaves the computer unattended they will ensure that the computer is locked first.

20.5 Where personal data held by the Company is used for marketing purposes, it is the responsibility of the Marketing department to seek authorisation from the Data Protection Officer who will ensure appropriate consent or legitimate interest is present (Part 3).

21 Data Security – IT Security

We promise to ensure that the following measures are taken in respect of IT Security:

21.1 All employees will receive unique credentials which shall not be shared with other employees, sub-contractors and third-parties. If a sub-contractor or third-party requires access to our system, they will be provided with a dedicated account provisioned using the principle of least privilege.

21.2 All software will be kept up-to-date, unless there are valid technical reasons for not doing so as determined by the IM&T department.

21.3 No software will be installed that is not approved by the IM&T department.

22 Transferring Personal Data to a Country Outside the EEA

We promise to limit the transfer of personal data outside of the EEA, and where this is necessary we shall only use third-parties that implement the GDPR compliant EU-US Privacy Shield Framework (https://www.privacyshield.gov/).

23 Data Breach Notification

We will do our best to prevent data breaches, however if a breach does occur we will follow the procedures below:

23.1 All personal data breaches will be reported to the Data Protection Officer.

23.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

23.3 If a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 23.2) to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.

23.4 Data breach notifications shall include the following information:

23.4.1 The categories and approximate number of data subjects concerned;

23.4.2 The categories and approximate number of personal data records concerned;

23.4.3 The name and contact details of the Company's Data Protection Officer (or other contact point where more information can be obtained);

23.4.4 The likely consequences of the breach;

23.4.5 Details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.