DATA PROTECTION POLICY

Goody Demolition
Wilcox Close
Aylesham Industrial Estate
Aylesham
Kent
CT3 3EP
T: 01304 840126
F: 01304 728351
E: info@goodydemolition.co.uk
W: www.goodydemolition.co.uk

Reviewed: 22-03-2021

Date of next review: 21-03-2022

Version: 2

Issue Number:	Date:	Comments:
001	16th July 2018	First Issue
002	21st May 2019	Addition of Change Log

Contents

1. Purpose

This document describes how, as a Data Controller, Goody Demolition aspires to the highest standards with regards to data protection and has been written to replace the existing Data Protection Policy (DPP) in order to bring Goody Demolitions data protection practices, procedures and processes in-line with the new General Data Protection Regulation (GDPR) which came into for on 25th May 2018.

The GDPR and its associated Bills supersede the Data Protection Act (DPA) 1998. It recognises additional rights to a data subject, tighter controls over the collection, use, storage and transfer (processing) of personal information (PI) and shifts the burden of accountability for the processing to the data controller and / or processor.

2. Definitions

2.1. 'We' means Goody Demolition as a company
2.2. Information owners: The individuals or departments within Goody Demolition that take responsibility for personal data.
2.3. Data controller: The entity (in this case, Goody Demolition) that determines the purposes and means of processing personal data.
2.4. Data processor: The entity that is responsible for processing personal data on behalf of a data controller.
2.5. Information Asset Register (IAR): This document serves as the basis of our personal data processing procedures. It specifies which data we store, how it is stored, how it is protected, with whom it is shared and the rights that data subjects have to it.
2.6. Information flow maps (DFMs): These documents show, visually, the path that our personal data takes as it enters, moves through and gets transferred from our company.
2.7. Information Update Register (IUR): This document provides an audit trail of updates that have occurred as a result of execution of a data subjects rights or an update that has occurred in the line of business. It allows us to prove that we have complied with a data subjects requests and affords us a level of data integrity that allows us to comply with the GDPR.
2.8. Privacy Impact Assessment (PIA): These documents will be created as required to evaluate the potential privacy impact to data subjects when employing new technologies within the business. They enable us to provide documented decisions which allow us to comply with the GDPR.
2.9. Privacy Notice: These documents provide notifications to data subjects with regards to the processing activities of and their rights to the personal data we hold and contacts details of the responsible party at Goody Demolition.
2.10. Data Breach Register (DBR): This document provides an audit trail of data breaches as required by law.

3. Policy

3.1. This policy applies to all staff of Goody Demolition Limited.
3.2. GDPR training will be regularly scheduled for both existing and new members of staff to ensure a current and complete knowledge of this policy across the organisation.
3.3. Any breach of this policy will be considered a disciplinary incident and appropriate action will be taken.
3.4. Any 3rd party that has access to the personal information we process are expected to read and comply with this policy.
3.5. Information owners inside the company, as detailed in the IAR, are expected to take responsibility to ensure that a contractual agreement between us as Data Controllers and any Data Processors exist which includes explicit clause(s) to ensure adherence to this policy and the GDPR.
3.6. All works contracts issued by us will include required clauses to ensure adherence to this policy and the GDPR.
3.7. This policy will be updated as required to reflect the evolution of the GDPR and data protection best practices.

Core Principles

The GDPR specifies that information will be processed according to 6 'Core Principles'. Goody demolition will adhere to these as follows:

"[Personal data will be] processed lawfully, fairly and in a transparent manner in relation to individuals"

3.8. Goody Demolition will make every reasonable effort to ensure that data subjects are informed of the data controller, the purpose of the processing, disclosures to 3rd parties, provided with the retention period for any data that will be kept and any other relevant information.

3.9. Our data repositories have been identified and audited to ensure compliance with the GDPR

3.9.1. An Information Asset Register (IAR) has been created and will be updated as required.

3.9.2. Information flow maps (DFMs) have been created that depict the lifecycle of the personal information that we process.

3.10. Information will always be processed fairly, with emphasis on the rights and freedoms of the data subject

3.11. Information will only be accessed under the context of its purpose as specified in the IAR

3.12. A Privacy Impact Assessment (PIA) will be undertaken whenever a new technology is employed throughout the business

3.12.1. The legal bases for the processing of the data will be weighed against the rights and freedoms of the data subject.

3.12.2. If the impact to the data subject will be potentially greater than the requirement to process the data then the technology not used

3.12.3. The results of the PIA will be used to create policies and procedures for the use of the new technology with data privacy at the forefront of consideration

3.13. Individuals will be made aware that we will be processing their information and why we will be processing it, at the initial point of data collection.

3.14. Job applicants will receive the Job Applicant Privacy Notice with each and every application form that will be sent out.

3.15. Employees will receive an Employee Privacy Notice when they commence employment with us.

3.16. Other data subjects will receive an email, letter or will otherwise directed to the General Privacy Notice displayed on our website.

3.17. CCTV notices will be clearly displayed around our offices and will be visible to visitors. These notices will contain a direction to our Privacy Policy on our website.

3.18. A Privacy Notice will always be accessible on our website.

"[Personal data will be] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial process"

3.19. Goody Demolition only processes personal information for the legal purpose it is initially collected for. This purpose is communicated to the data subject upon collection.

3.20. The processing activities of personal information are recorded in the IAR which documents the following:

3.20.1. Which personal data are processed

3.20.2. The reason for processing
3.20.3. The legal basis for processing each personal data and where required the basis under Article 9 for processing special category data
3.20.4. The individual or business role responsible for the data
3.20.5. The general format of the data
3.20.6. The categories of individuals to which the data applies
3.20.7. Whether the data is ever transferred to a non-EU country
3.20.8. Whether consent is required for the processing of the data and if it has been obtained
3.20.9. Whether the data is shared with a 3rd party
3.20.10. The data retention period
3.20.11. The location of the data

3.21. If we determine the most suitable legal basis for the processing of personal information will be one of legitimate interest, a Legitimate Interest Assessment (LIA) will be undertaken in order to compare our interests to that of the data subject.
3.22. Where our interests could be overridden by the data subjects' rights or freedoms, a risk analysis will be performed to measure the likelihood of the infringement of the data subjects' rights or freedoms.
3.22.1. The decision to process the data will be made based on the outcome of the risk analysis; should it show anything other than a low risk, the data is not processed.
3.22.2. Any LIAs will be kept alongside the IAR to provide documentation of our decisions.
3.23. We will never process information for any purpose other than the purpose defined, including for the allowable exceptions specified in the principle

---

"[Personal data will be] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

3.24. Goody Demolition only stores personal information that will be required to fulfil its purpose, as defined in the IAR.
3.25. Information collection procedures identified in the IAR are regularly audited to ensure the collected information is required and relevant

---

"[Personal data will be] accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"

3.26. An information update request is sent to data subjects every year to ensure we hold the correct information for them
3.26.1. Personal information is never sent with this request
3.26.2. The request is time-limited; if we do not receive a reply within 4 weeks then the information is deemed out-of-date and is removed in compliance with this policy
3.27. Information identified as not required or relevant will be removed from the collection methods and methodically erased throughout the organisations historical records
3.28. Using the IAR and our DFMs, we will identify where the information resides
3.29. Information will be securely erased from any current stores
3.30. An Information Update Register (IUR) will be kept to reflect the updates made to ensure, in the event of backup restoration, the old data will not made current

3.30.1. Information registered in the IUR will be given a 365-day expiry date, in-line with the age of our data backups
3.30.2. The IUR will be regularly audited to remove expired entries
3.30.3. Upon data backup restoration, the IUR will be applied to the restored data to bring it up-to-date

3.31. Any updated information will be passed to relevant 3rd parties to ensure their data for the data subject is also updated and correct.
3.32. We will identify the 3rd party recipients of our personal information using our DFMs and IAR.

"[Personal data will be] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals"

3.33. Retention periods for the various types of personal information are recorded in the IAR.
3.34. We will not store personal information, in any way, once its' purpose is no longer valid.
3.35. Expired information is securely removed in compliance with this policy.
3.36. Expired information will removed from any relevant 3rd parties' databases after identifying those 3rd parties using our information flow maps.

"[Personal information will be] processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

3.37. Physical records that contain personal information are always kept in a secure, locked filing area.
3.38. Access to secure filing areas is controlled by the Admin management and the HR management teams.
3.39. Only authorised personnel are granted access to secure filing areas.
3.40. Access to digital records that contain personal information is controlled via Access Control Lists (ACLs).
3.41. ACL memberships are authorised and reviewed by management on the schedule defined by our Control of IT Systems policy.
3.42. Encryption is employed where appropriate to secure digital communications.
3.43. The IT use policy defines the security measures we use to ensure access to digital systems to authorised employees.
3.44. The IT use policy defines the methods available for transferring information and the procedures for doing so.
3.45. Goody Demolition has attained the Cyber Essentials Certificate therefore its' IT systems comply with the certification security, process and management requirements.
3.46. Goody Demolition has attained and is governed by the ISO 9001 management system certification. Additional policies and procedures defined in our ISO 9001 management system demonstrate our commitment to general information security throughout the organisation.

Data Protection Officials

3.47. The responsible party for any and all Data Protection enquiries is the HR management team.

3.48. All requests and enquiries regarding data protection will be directed to the HR management team.
3.49. We have determined that there is no requirement to appoint a Data Protection Officer based on the following reasons:
    3.49.1. We are not a public authority
    3.49.2. Our core activities do not require large scale, regular and systematic monitoring of individuals
    3.49.3. Although we do process information relating to criminal convictions and special category information, our core activities do not comprise these activities

International Transfers

3.50. Where practical and preventable, we will never transfer personal information outside of the EU.
3.51. When information is transferred within the EU, the transfer must take place in compliance with this policy, adhering to security and privacy standards and practices whenever possible.
3.52. When information transfers outside the EU are unavoidable, every effort must be made to ensure the recipient of the information complies with the security and privacy standards and practices defined in this policy and / or demonstrates an adequate level of information protection compliance, for example the US Privacy Shield program.

Data Subject Rights

Data subjects have various rights to their personal information held by us.

3.53. Details of which right applies to which information are recorded in the IAR.
3.54. Any initiation of a request must be made in accordance with the procedure on the Privacy Notice to which the data subject applies.
3.55. Requests must be completed within 28 days following receipt of the request.
3.56. The secure transfer of the response must be made in compliance with this policy and where appropriate, the IT use policy.
3.57. Information that is held for a data subject can be identified on the IAR.
3.58. If a request is unfounded, excessive or repetitive, a fee will be charged to cover administration costs. The level of this fee is at the discretion of the management team but will be reasonable.
3.59. Any response when a fee has been charged must include:
    3.59.1. The reason for the fee
    3.59.2. Their right to complain to the ICO or other supervisory authority
    3.59.3. Their ability to seek to enforce this right through a judicial remedy
3.60. Any response when a request has been refused must include:
    3.60.1. The reason for the refusal
    3.60.2. The data subjects' right to complain to the ICO or other supervisory authority
    3.60.3. The data subjects' ability to seek to enforce this right through a judicial remedy
3.61. Any information erasures as a result of any request must be performed in compliance with this policy.

Information Disclosures

3.62. All information disclosures to data processors, joint data controllers or data subjects will comply with this policy.
3.63. Information will never be disclosed to any 3rd party other than those that lawfully require it.
3.64. Information disclosures must be handled according to our information disclosure procedure (section 4.2)

Data Breaches

3.65. Once detected, data breaches must be handled according to our data breach procedure (section 4.4).
3.66. A report to the ICO must be made within 72 hours following the discovery of the data breach where the breach may moderately (or higher) affect a data subject.

3.66.1. Responsible staff must fill in a Data Breach form, available from the ICOs website: https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc

3.66.2. Keep the copy of the completed form in the data breach forms folder

3.66.3. Call the ICO on 0303 123 1113 and provide them with the information on the form or send the completed form to the email address specified on the form

3.67. Any data breach that can potentially and adversely affect a data subjects' rights and freedoms must be reported to the data subject without undue delay.

3.68. Responsible staff must complete a risk assessment to identify if there is a need to notify the data subject.

3.68.1. The risk assessment must evaluate the likelihood and severity of the breach on the data subject.

3.68.2. When the risk that the likelihood or severity is substantial, a Goody Demolition data breach form will be completed and sent to each data subject to which the breach concerns.

3.69. Any data breach must be recorded in the Data Breach Register.

3.70. Training will be provided to staff members to enhance their awareness of data breaches and the methods that they must use to detect and report them.

3.71. Deliberate, unauthorised access or alteration to personal information held by us by our employees will be classed as gross misconduct and will be handled according to our employment policy.

4. Procedures

4.1. Data Subject rights

4.1.1. Access

4.1.1.1. Verify the recipient of the requested data before sending it. Record the result of the check in the Rights execution register.

4.1.1.2. Enter the details of the request in the Rights Execution register spreadsheet.

4.1.1.3. Gain authorisation for the request from a member of the management team.

4.1.1.4. Identify the method of transfer that will most suitably uphold the data subject's right of portability.

4.1.1.5. Ensure, where applicable, the data requested is transferred adhering to this policy and the Information Disclosures procedure.

4.1.1.6. Record the data transfer in the Data Transfers register spreadsheet

4.1.2. Rectification and erasure.

4.1.2.1. Verify the identity of the individual making the request.

4.1.2.2. Enter the details of the request in the Rights Execution Register spreadsheet.

4.1.2.3. Gain authorisation for the request from a member of the management team.

4.1.2.4. Using the IAR and the Data Transfers register, identify to which 3rd parties the data has been transferred.

4.1.2.5. Inform any 3rd parties of the update to the personal data, adhering to this policy and the Information Transfers procedure.

4.1.2.6. Record the data transfer in the Data Transfers register spreadsheet.

4.1.2.7. Record the data update in the data update register spreadsheet. Ensure the ID for the record is entered into the corresponding entry in the rights execution register.

4.1.3. Objection

4.1.3.1. Verify the identity of the individual making the request. Record the result of the check in the Rights execution register.

4.1.3.2. Enter the details of the request in the Rights Execution Register spreadsheet.

4.1.3.3. Gain authorisation for the objection from a member of the management team.

4.1.3.4. Where the result of an objection is a data update or erasure, refer to 4.1.2.

4.2. Information Transfers

4.2.1. Verify the identity of the recipient of the personal data

4.2.2. Where applicable, verify the recipient has adequate data protection measures in-place and is GDPR compliant

4.2.3. Where possible, transfer the data digitally as this will most suitably uphold the data subject's right of portability.

4.2.4. Transfer the data securely, in compliance with this policy. Refer to the IT use policy for details regarding the secure transfer of digital information.

4.2.5. Record the transfer in the Data Transfers spreadsheet

4.3. Transfers Outside the EU

4.3.1. Verify the validity of the recipient's data protection measures and that they are compliant with GDPR derogations (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/).

4.3.1. Note the derogation reason from the ICO website for the transfer on the Data Transfer spreadsheet.

4.3.2. Follow the Information Transfers procedure (4.2)

4.4. Data Breaches

4.4.1. Notify the data protection management individual of the data breach.

4.4.2. Record the details of the breach using the data breach form.

4.4.3. Save the form using a unique filename.

4.4.4. Perform a risk analysis to identify the likelihood that the breach will affect the concerned data subjects and the potential severity of the breach on the data subject.

4.4.5. Save the risk analysis using a unique filename.

4.4.6. If the likelihood that the breach will affect the data subject is moderate or above then inform the data subject by securely verifying their contact details and then forwarding the data breach form to them using a transfer method that complies with this policy.

4.4.7. If the potential severity of the breach to the data subject is moderate or above, the ICO must be informed using the online form (section 3.66.1).

4.4.8. File the data breach form and the completed risk analysis in the completed data breach forms folder and completed risk analyses folder, respectively.

4.4.9. Obtain authorisation from a management team member.

Latest Review Dated **22 April 2021**

Signed By

Managing Director

Gary Venner