Data Protection Policy

Great White Destruction Ltd

Contents

Executive Summary

This policy has been developed to ensure compliance with all regulations relating to data protection namely:

- Data Protection Acts, 1988 and 2003 (as amended)
- General Data Protection Regulation (25 May 2018)

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Acts 1988 and 2003 and from 25 May 2018 the General Data Protection Regulations confer rights on individuals as well as responsibilities on those persons processing personal data.

Great White Destruction Ltd (GWDL) collects and uses personal data about its staff, stakeholders and other individuals who come in contact with the company, for a variety of purposes. This data is collected when GWDL can rely on one of the legal grounds for processing and the data subject is provided with all information to which a data subject must be provided with under data protection laws.

We treat all personal data as confidential.

To this end a policy has been produced detailing the:

- Definitions of relevant terms
- Governing principles of personal data protection
- Procedure for dealing with personal data access requests
- Procedure for dealing with data loss
- Procedure for dealing with data breaches

Data includes, but is not limited to, any record, document, file, data or other form of information that is created, held, stored or shared by any means and includes, but is not limited to:

- Electronic data
- CCTV footage
- Paper-based information (eg reports, letters, records, faxes and other documents)
- Information communicated via emails or on a computer screen

This document will be reviewed regularly in light of any legislative or other relevant indicators, and amended as needed.

Data Protection Policy

Data Protection Compliance Manager: David Walsh

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our stakeholders, employees, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf.

2. ABOUT THIS POLICY

2.1 The types of personal data that GWDL may be required to handle include information about current, past and prospective suppliers, stakeholders, employees and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Acts 1988 and 2003 (**the Acts**) (and with effect from the 25 May 2018 the General Data Protection Regulation (**GDPR**)) and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** means data processed wholly or partly for automated means or manually where it forms part of a relevant filing system or is intended to form part of a relevant filing system.

3.2 **Data subjects** means a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

3.3 **Personal data** means any information relating to an identified or identifiable natural person (data subject), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identification identifier or to one or more factors specific to the physical physiological, genetic, mental, economic, cultural or social identity of that natural person .

3.4 **Data controllers** are those who determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Acts. We are the data controller of all personal data used in our business for our own commercial

purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** are persons or entities who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract (which should be on the basis of a formal written contract), but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Special Categories of Personal Data** Personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, genetic data, biometric data and biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specific, explicit and legitimate purposes and not further processed in any manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;
- Accurate, and where necessary, kept up to date;
- Not kept longer than necessary for the purpose;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical organisational measures
- Processed in accordance with the Data subjects' rights, including the right of access, the rectification, the right to erasure (*"the right to be forgotten"*) the right to restriction of

processing, and the right to object to processing and the right to data portability.

- Not transferred to people or organisations situated in countries outside the EEA without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Acts and the GDPR are not intended to prevent the processing of personal data, but to ensure that it is done fairly, transparently and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Acts and from 25 May 2018, the GDRP. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest pursued by the data controller or the party except where such interests are over ridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Special Categories of Personal Data and data relating to criminal convictions can only be processed, when specific conditions are met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for specific purposes or for any other purposes specifically permitted by the Acts and the GDPR once implemented. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7**.1** If we collect personal data directly from data subjects, we will inform them about:

- Our identity and contact details;
- The purposes or purposes for which we intend to process that personal data, as well as the legal basis for the processing;
- The categories of personal data concerned;
- The types of third parties, if any, with which we will share or to which we will disclose that personal data;

Additionally, with effect from the implementation of the GDPR on 25th May 2018, we will inform data

subjects:

- That the processing is based on the legitimate interests pursued by the data controller;

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine the period**;**

- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability

- Where the processing is based on consent, the existence of the right to withdraw consent at any time, without effecting the lawfulness of the processing based on consent before withdrawal.

- The right to lodge a complaint with the Office of the Data Protection Commissioner;

- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- The existence of automate decision making, including profiling and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter and the source from which the personal data originated, and if applicable whether it came from public accessible sources.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the Data Protection Compliance Manager is.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

9.1 We will strive to ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

10.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller;
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended;
- The right to restriction of processing;
- The right to be forgotten;
- The right to data portability, upon the implementation of the general Data Protection Regulation;
- The right to object to the processing.

12. DATA SECURITY

12.1 We will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of any breach.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the central computer system instead of individual PCs.

12.4 Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

- **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

- **Encryption:** All laptops, flash drives and smart phones to be encrypted.

- **Backup:** All critical systems and data are backed up off site on a daily basis

- **Firewall:** Best in class Cisco ASA firewall protects our network from external intrusion.

- **Anti-virus:** Centralised anti-virus solution on all hardware

- **Education:** Regular briefings to staff on cyber security risks and threats

13. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

13.1 GWDL will only share information with third parties where it is necessary in order to meet statutory or contractual obligations of the organisation.

These reasons include, but are not limited to:

- **Remuneration and other financial arrangements with staff**
- **Receipt of payments from customers**
- **Payments to product and service providers**

14. DEALING WITH DATA SUBJECT RIGHTS AND REQUESTS

14.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their line manager in the first instance and thereafter to the Data Protection Compliance Manager immediately. See Appendix 2 – Access Request Form

14.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14.3 Our employees will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees will not be bullied into disclosing personal information.

14.4 Data subjects have rights when it comes to how we handle their personal data. These rights include**;**

a) The right to withdraw consent to processing at any time
b) Receive certain information about the data controllers processing activity
c) Request access to their personal data that we hold
d) Prevent our use of their personal data for direct marketing purposes
e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete data
f) Restrict processing in specific circumstances
g) Challenge processing that has been justified on the basis of legitimate interest or public interest
h) Request a copy of an agreement under which personal data is transferred outside of the European economic area
i) Object to decisions based solely on automated processing, including profiling
j) Prevent processing that is likely to cause damage or distress to the data subject or anybody else
k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
l) Make a complaint to the data protection commissioner
m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used machine readable format (the right to data portability)

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you to disclose personal information without proper authorisation).

You must immediately forward any data subject request to the data protection compliance manager immediately. In the case of a data access request the data access request form set out at appendix 2 can be used.

15. DATA BREACH

15.1 All Data breaches are to be reported without delay to the relevant line manager and in turn to the Data Protection Compliance Manager. From the 25 May 2018 once the GDPR is implemented, we will log all personal data breaches. Where ascertained that the data breach poses a risk to the individuals involved the office of the data protection commissioner will be informed within 72 hours of breach discovery. Depending on the circumstances of the breach we may also notify the data subject or subjects without undue delay. See Appendix 2 – Data Security Breaches

Schedule of Data Types

Type of data	**Data subjects**	**Retention period**
• Employee and stakeholder contact names and addresses • Employee and stakeholder phone and emails • Employee and stakeholder financial details • CCTV data	• Employee • Stakeholder • Supplier	Personal data is collected for specific purposes and is retained only for as long as there is a legal basis to do so. Eg Employee 7 years post employment Stakeholder /Supplier subject to specific business arrangement Personal Data Periods under continuous review.

Data Loss Notification Procedure

Introduction:
The purpose of this document is to provide a concise procedure to be followed in the event that GWDL becomes aware of a loss of personal data. This includes obligations under law, namely the
Irish Data Protection Acts (1988 and 2003),) and as of 25 May 2018 the General Data Protection Regulation.

Rationale:
The response to any breach of personal data can have a serious impact on GWDL's reputation and the extent to which the public perceives GWDL as trustworthy.

The consequential impact on the commercial brand can be immeasurable. Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification. This guide is to assist staff in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Scope:
The policy covers both personal and sensitive personal data held by GWDL. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by GWDL. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

What constitutes a breach, potential or actual?
A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on pc's and applications
- Emailing a list of personal data to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?
Actual, suspected, or potential breaches should be reported immediately to the relevant line manager who will in turn inform the Data Protection Compliance Manager (DPCM).

A team comprising the DPCM, Manager and other relevant staff will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection if required.

In certain circumstances GWDL may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. GWDL will make recommendations to the data subjects which may minimise the risks to them. GWDL will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

When will the Office of the Data Protection Commissioner be informed?
GWDL will, without undue delay and where feasible not later than 72 hours after having become aware of it notify the data breach to the data protection commissioner unless the personal data breach is unlikely to result in a risk to the rights and freedoms of a natural person.

When the data breach is likely to result in a high risk to the rights and freedoms of an individual, we will communicate the personal data breach to that individual without undue delay.

Data Loss Incident logging.
All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and indicated if the Data Protection Commissioner and/or the data subject was informed and if there were not an explanation of the rationale for not reporting the breach Such records will be provided to the Office of the Data
Protection Commissioner upon request. See Appendix 4 – Sample Data Breach Log

Appendix 1 – Access Request Form

Personal Data Access Request Form

Section A – please complete this section

Full Name…….

Postal Address……
……
……
……
……

Telephone/e-mail*

……(include area code)
*We may need to contact you to discuss your Access Request

Please return this form to: **Great White Destruction Ltd, Units 1D-2B Enterprise Centre, Summerhill, Co. Meath, A83 XR70**

Section B – please complete this section

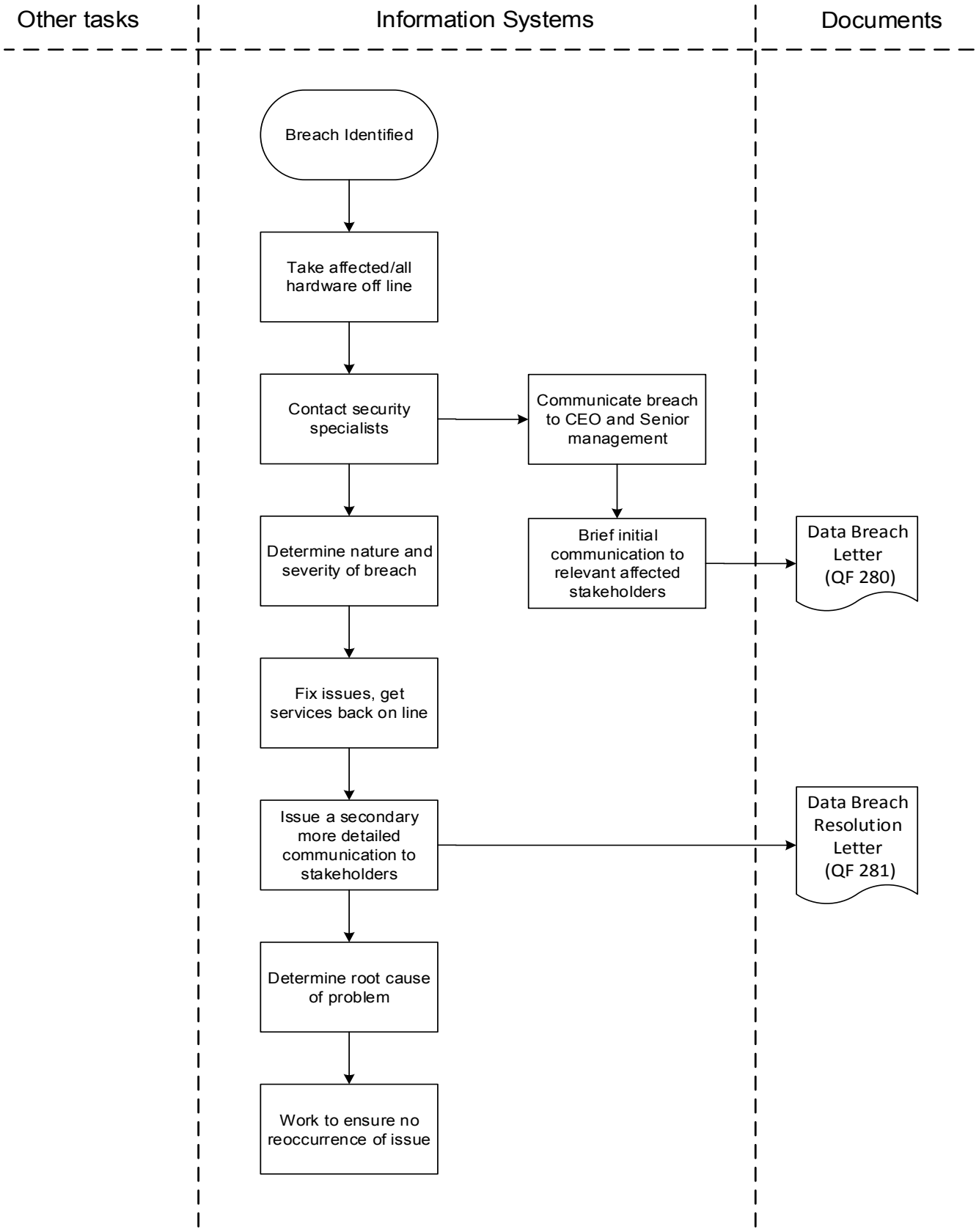
I, …….(insert name) wish to have access to data that I believe Great White Destruction Ltd retains on me as outlined below

……
……
……
……
……
……
……
……..

Signed…… Date……..

For office use only
_____
_____
_____
_____

Appendix 2 – Data Security Breaches (WI 160) Quality Management system



Data breach notification letter template (QF 280)

To: Data Subject

Date

Dear

We are contacting you because we have learned of a data security incident that occurred on (specific or approximate date) OR between (date, year and date, year) that may have involved some of your business information.

The breach involved (provides a brief general description of the breach and include how many records or businesses it may have affected). The information breached contained (names, contact details, other information). Other information (provide details) was not released.

The likely consequences of the personal data breach are [ ].

For further information please contact [ ].

[Insert description of measures taken or proposed to be taken to address the personal data breach, including measures to mitigate its possible adverse effect].

We are notifying you so you can take whatever action as may be required to protect your own security.

I can assure you that GWDL is doing its utmost to identify the source of the breach and to ensure that protective measures are put in place to prevent any further breaches.

GWDL is fully committed that all of its employees comply with any notification requirements under the Data Protection Acts 1988 and 2003 and the General Data Protection Regulation, and that GWDL will duly observe all its obligations under the Data Protection Acts 1988 and 2003 and the General Data Protection Regulation which may arise in connection with the scheme.

If you have further questions or concerns, you may contact the undersigned at this special telephone number: 046-9557508. You can also check our website at www.greatwhite.ie for updated information.

Signed (for GWDL)

Data breach resolution letter (QF 281 V.1)

To: Data Subject

Date

Dear

As per our previous correspondence dated (insert date) GWDL's systems have fallen victim to a security breach.

GWDL has always taken the security of your data very seriously and has strived to ensure this security.

However, in light of recent events the following actions have been taken to enhance cyber security.

(List of measures taken in light of breach)

Once again I would like to reassert out commitment to security and assure you that we are taking all possible measures to ensure such an incident will not reoccur.

Signed (for GWDL)

Appendix 3 – On line privacy policy

http://www.greatwhite.ie/documents.asp

This statement relates to our privacy practices in connection with this website. We are not responsible for the content or privacy practices of other websites. Any external links to other websites are clearly identifiable as such. Some technical terms used in this statement are explained at the end of this page.

General statement
GWDL fully respects your right to privacy, and will not collect any personal information about you on this website without your clear participation and permission. Any personal information which GWDL requires will be treated with the highest standards of security and confidentiality, strictly in accordance with the Data Protection Acts, 1988 & 2003.

Collection and use of personal information
GWDL will only collect personal information via forms that you may be asked to complete. Any information which you provide in this way is not made available to any third parties, and is used by GWDL only in line with the purpose for which you provided it.

Requests regarding data supplied via this website
On request, we supply copies of your personal data which you may have supplied via this website. If you wish to obtain such copies, you must write to GWDL at the address below, or e-mail us at david@greatwhite.ie. You should include any personal identifiers which you supplied earlier via the website (e.g. Name; address; phone number; e-mail address). Your request will be dealt with as soon as possible and will take not more than 40 days to process.

If you discover that GWDL holds inaccurate information about you, you can request the information be corrected. Such a request must be in writing or via e-mail.

Complaints about data processed via the website
If you are concerned about how personal data are processed via this website, please do not hesitate to bring such concerns to the attention of GWDL at the contact details below.

Updates
Our Privacy Policy may change from time to time and all updates will be posted on this page.

Appendix 4 – Sample Data Breach Log

All data breaches will be logged in summary form in the Data Breach Log. Any data breaches deemed by GWDL to be severe will be notified to the Office of the Data Commissioner within 72 hrs in accordance with General Data Protection Regulations and the relevant Acts.

Department Involved	No. of Individuals affected	Date of Breach	Was the breach reported? (Y/N)	If not why?	Resolution