Henry Boot

Data protection policy

V9, 2024

Applicable to:
All persons within the Henry Boot group

Produced by:
A. Stanbridge, Data Privacy Manager

Effective from:
March 2024

Policy/Guidance Number:
Pol.9 (V9)

To be reviewed by:
February 2025

Staff responsible for revision:
Data Privacy Manager

Linked documents:
Information systems and security policy
Social media policy
Document management policy

Versions:
Version 1 – March 2002
Version 2 – April 2012
Version 3 – June 2015
Version 4 – May 2018
Version 5 – January 2020
Version 6 – February 2021
Version 7 – February 2022
Version 8 – February 2023
Version 9 – March 2024

Signed by:
T.A. Roberts, Chief Executive Officer

Overview

This policy aims to clarify our commitment to complying with all aspects of data protection legislation in our handling of personal information in relation to customers, suppliers and employees. The Data Privacy Manager is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines. Henry Boot adheres to all principles relating to the processing of personal data, as set out in the UK GDPR, and has put in place many measures to assist in the implementation of these principles, as set out in this policy.

Contents

1. Policy statement

1.1. We are committed to complying with all aspects of the data protection legislation in our handling of personal information in relation to customers, suppliers and employees. Henry Boot's policy is to ensure that such information is only stored, processed and disclosed when business needs require it and, where necessary, to supply privacy notices to and obtain all appropriate consents from individuals who are the subject of such information. We are also committed to allowing individuals appropriate access to information held about them and to a regular process of updating and/or destroying out of date information.

1.2. This policy applies to all personal data processed by Henry Boot, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.

1.3. This policy applies to all Henry Boot employees. You must read, understand and comply with this policy when processing personal data on our behalf and undertake training on its requirements. This policy sets out what we expect from you in order for us to comply with applicable law. Your compliance with this policy is mandatory. Related policies and privacy guidelines are available to help you interpret and act in accordance with this policy. You must also comply with all related policies and privacy guidelines. Any breach of this policy may result in disciplinary action.

1.4. This policy (together with related policies and privacy guidelines) is an internal document and can't be shared with third parties, clients or regulators without prior authorisation from the Data Privacy Manager (DPM).

2. Aims of this policy

2.1. To operate our business effectively, we need to obtain, use and store information about our customers, suppliers and employees. Data protection legislation controls and limits the collection and use of information which relates to and identifies any person, which is described as personal data. Both computerised information and paper-based records are covered, provided that the relevant information is filed by reference to that person (ie. in a file with their name or employee number on it). We are committed to best practice in this area and the aims of this policy are threefold:

- To educate employees in relation to our approach to handling personal data
- To explain the various requirements of the UK GDPR, being the retained version of the EU General Data Protection Regulation 2016 as tailored by the Data Protection Act 2018 (DPA) and associated legislation, and
- To explain to employees what is expected of them in relation to data protection.

3. Scope

3.1. We recognise that the correct and lawful treatment of personal data will maintain confidence in Henry Boot and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. We are exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

3.2. All managers are responsible for ensuring that all employees comply with this policy, They must implement appropriate practices, processes, controls and training to ensure this compliance.

3.3. The DPM is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines. That post is held by Amy Stanbridge, General Counsel and Company Secretary, astanbridge@henryboot.co.uk.

3.4. Please contact the DPM with any questions about the operation of this policy or the UK GDPR, or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPM in the following circumstances:

a) If you are unsure of the lawful basis on which you are relying to process personal data (including the legitimate interests used by the group, plus also see Schedule 1).

b) If you need to rely on consent and/or need to capture explicit consent to process personal data.

c) If you need to draft privacy notices or fair processing notices.

d) If you are unsure about the retention period for the personal data being processed (plus also refer to our document management policy).

e) If you are unsure what security or other measures you need to implement in order to protect personal data (plus refer to the group's IT team and the information systems and security policy).

f) If there has been a personal data breach (plus refer to Schedule 3).

g) If you are unsure on what basis to transfer personal data outside the UK.

h) If you need any assistance dealing with any rights invoked by a data subject (plus also see Schedule 2).

i) Whenever you are engaging in a significant new, or change in, processing activity likely to require a Data Protection Impact Assessment (DPIA) or you plan to use personal data for purposes others than for what it was collected for.

j) If you plan to undertake any activities involving automated processing including profiling or automated decision-making.

k) If you need help complying with applicable law when carrying out direct marketing activities.

l) If you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors).

3.5. Disciplinary action in accordance with our disciplinary and dismissal procedure may be taken against any employee who breaches any of the instructions or procedures following from this policy.

4. Implementation of data principles

4.1. We adhere to the principles relating to processing of personal data, as set out in the UK GDPR, which require personal data to be:

a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).

b) Collected only for specified, explicit and legitimate purposes (purpose limitation).

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation).

d) Accurate and, where necessary, kept up to date (accuracy).

e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (storage limitation).

f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (security, integrity and confidentiality).

g) Not transferred to another country without appropriate safeguards being in place (transfer limitation).

h) Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (data subject's rights and requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

These principles and our compliance with them – our accountability – are set out in more detail in paragraph six (below) and Schedule 1 to this policy.

4.2. In order to assist in the implementation of these principles and with the UK GDPR more generally, we have:

a) Carried out a data protection audit, and produced corresponding audit and implementation reports, detailing the measures put in place to comply with the UK GDPR.

b) Produced a written record of processing activity in accordance with Article 30 of the UK GDPR.

c) Appointed a DPM with specific responsibility for the implementation of the data protection principles, who has been nominated as the person to whom all queries in relation to data protection matters should be directed.

d) Updated all contracts with relevant suppliers to include UK GDPR-compliant clauses and ensure that suppliers put in place all appropriate measures to assist us with our own UK GDPR compliance.

e) Implemented a number of additional IT security measures and related upgrades to relevant software and database packages to ensure ease of compliance with the UK GDPR and, in particular, data subject requests.

f) Put in place systems of mandatory e-learning in relation to data protection and cyber security issues.

g) Prepared updated privacy notices to be provided to any individual whose personal data is processed by us.

h) Put in place systems of data storage that will ensure data is held with an appropriate degree of security, that data will only be accessed where strictly necessary and only by those with authority to do so.

Appropriate efforts will be made to ensure that all stored data is accurate and updated as necessary and that data which is obsolete or no longer required is destroyed with appropriate regard paid to the confidentiality of that information. Relevant to this are the linked policies:

- Document management policy: Sets out the retention period for documents that may include personal data
- Information systems and security policy: Sets out security measures relating to electronic data storage and transfer.

4.3. Further details of these measures, and their implementation, can be found in our UK GDPR implementation report, which is available on request from the DPM.

5. Data subjects rights and requests

5.1. Data subjects have rights when it comes to how we handle their personal data. These include rights to:

a) Withdraw consent to processing at any time

b) Receive certain information about the data controller's processing activities

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's no longer necessary in relation to the purposes for which it was collected or processed, or to rectify inaccurate data or to complete incomplete data

f) Restrict processing in specific circumstances

g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest

h) Request a copy of an agreement under which personal data is transferred outside of the UK

i) Object to decisions based solely on automated processing, including profiling (ADM)

j) Prevent processing that is likely to cause damage or distress to the data subject or anyone 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 supervisory authority, and

m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

The procedures for dealing with the above are set out in Schedule 2 to this policy.

5.2. 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 into disclosing personal data without proper authorisation).

5.3. You must immediately forward any data subject request you receive to the DPM.

6. Accountability

6.1. We are required to implement appropriate technical and organisational measures in an effective manner, to ensure compliance with the data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles set out at paragraph four and Schedule 1.

We must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

a. Appointing a suitably qualified DPM and an executive accountable for data privacy.

b. Implementing privacy by design when processing personal data and completing Data Protection Impact Assessment (DPIAs) where processing presents a high risk to rights and freedoms of data subjects.

c. Integrating data protection into internal documents including this policy, related policies, privacy guidelines, privacy notices or fair processing notices.

d. Regularly training employees on the UK GDPR, this policy, related policies, privacy guidelines, and data protection matters including, for example, data subjects' rights, consent, legal basis, DPIA and personal data breaches. We must maintain a record of training attendance by employees.

e. Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

6.2. Processing

All processing of personal data must be done in accordance with the data protection principles and the procedures and requirements set out in this policy.

6.3. Record keeping

The UK GDPR requires us to keep full and accurate records of all our data processing activities.

As set out in paragraph four, we are required to maintain a written record of processing activity. If you become aware of any personal data being processed which you don't believe is on the written record, you should notify the DPM. In addition, we are required to keep and maintain accurate corporate records of data subjects' consents and procedures for obtaining consents if we ask for them from any individuals. Should you need to obtain consent from an individual to process their personal data, please contact the DPM, who can advise on the best form for obtaining consents and providing relevant privacy/fair processing notices.

6.4. Training and audit

We are required to ensure all employees have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training provided by us.

You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

6.5. Privacy by design and Data Protection Impact Assessment (DPA)

We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

A DPIA will need to be carried out when implementing major system or business change programs involving the processing of personal data including:

a. Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes)

b. Automated processing including profiling and ADM

c. Large-scale processing of special categories of personal data, and

d. Large-scale, systematic monitoring of a publicly accessible area.

Please contact the DPM if any of the above applies to any measure you are proposing to introduce, to advise on the carrying out of a DPIA.

A DPIA will include:

a. A description of the processing, its purposes and the data controller's legitimate interests if appropriate

b. An assessment of the necessity and proportionality of the processing in relation to its purpose

c. An assessment of the risk to individuals, and

d. The risk mitigation measures in place and demonstration of compliance.

6.6. Automated processing (including profiling) and Automated Decision-Making (ADM)

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual, unless:

a. The data subject has provided explicit consent

b. The processing is authorised by law, or

c. The processing is necessary for the performance of or entering into a contract.

We don’t envisage a circumstance in which ADM will be required for any of our processing activities. However, if you identify the need for ADM, please contact the DPM.

6.7. Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

6.8. Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related “need to know” the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the personal data we hold with third parties, such as our service providers, if:

a) They have a need to know the information for the purposes of providing the contracted services

b) Sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained

c) The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place

d) The transfer complies with any applicable cross border transfer restrictions, and

e) A fully executed written contract that contains UK GDPR-approved third-party clauses has been obtained.

Please contact the DPM if you have any queries about whether data sharing should be carried out.

7. Schedule 1 – Data protection principles and their implementation

1. Lawfulness, fairness and transparency

1.1 Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We may only collect, process and share personal data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but to ensure that we process personal data fairly and without adversely affecting the data subject.

The UK GDPR allows processing for specific purposes, some of which are set out below:

a) The data subject has given his or her consent

b) The processing is necessary for the performance of a contract with the data subject

c) To meet our legal compliance obligations

d) To protect the data subject's vital interests, and

e) To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices or fair processing notices.

You must identify and document the legal ground being relied on for each processing activity in accordance with the categories above. if you have any queries about this, contact the DPM.

1.2 Consent

A data controller must only process personal data on the basis of one or more of the lawful bases set out in the UK GDPR, which include consent.

A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

Unless we can rely on another legal basis of processing, explicit consent is usually required for processing special categories of personal data, for automated decision-making and for cross border data transfers. Usually, we will be relying on another legal basis (and not require explicit consent) to process most types of special categories of personal data. Where explicit consent is required, we must issue a fair processing notice to the data subject to capture explicit consent.

You will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

1.3 Transparency (notifying data subjects)

The UK GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate privacy notices or fair processing notices which must be concise, transparent, intelligible, easily accessible, and in clear, plain language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with all the information required by the UK GDPR including the identity of the data controller and DPM, how and why we will use, process, disclose, protect and retain that personal data through a fair processing notice which must be presented when the data subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the data subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. You must also check that the personal data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed processing of that personal data.

If you require a privacy notice/fair processing notice, contact the DPM.

2. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

3. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

You may only collect personal data that you require for your job duties. Do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines, as set out in the document management policy.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You must ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data, in accordance with the data retention guidelines set out in the document management policy.

5. Storage limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

We have retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held unless a law requires such data to be kept for a minimum time. You must comply with our document management policy which relates to data retention.

You will take all reasonable steps to destroy or erase from our systems all personal data we no longer require in accordance with all our applicable records, retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice or fair processing notice.

6. Security integrity and confidentiality

6.1 Protecting personal data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We have developed, implemented and will maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others, and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal data we hold.

You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting special categories of personal data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

d) You must comply with all applicable aspects of our Information systems and security policy which contains administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect personal data.

6.2 Reporting a personal data breach

The UK GDPR requires data controllers to notify any personal data breach to the applicable regulator, and, in certain instances, the data subject. We have put in place procedures to deal with any suspected personal data breach (see Schedule 3 of this policy) and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately follow the procedure set out in Schedule 3. You should preserve all evidence relating to the potential personal data breach.

7. Transfer limitation

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer personal data outside the UK if one of the following conditions applies:

a) The UK has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms.

b) Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPM.

c) The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks.

d) The transfer is necessary for one of the other reasons set out in the UK GDPR, including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims, or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

If such a transfer will be taking place, contact the DPM to ensure the appropriate contractual safeguards are put in place in relation to that transfer.

8. Schedule 2 – Response procedures for data subject requests

1. About these procedures

1.1 Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. These procedures provide a framework for responding to requests to exercise those rights. It is our policy to ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law.

1.2 These procedures only apply to data subjects whose personal data we process.

2. Responding to requests to access personal data

2.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs).

When a data subject makes an SAR we shall take the following steps:

a) Log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met).

b) Confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity.

c) Search databases, systems, applications and other places where the personal data which are the subject of the request may be held,

d) Confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.

2.2 If personal data of the data subject is being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

a) The purposes of the processing.

b) The categories of personal data concerned (for example, contact details, bank account information and details of sales activity).

c) The recipients or categories of recipient to whom the personal data has or will be disclosed, in particular recipients overseas (for example, US-based service providers).

d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period – usually by reference to the group document management policy.

e) The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing.

f) The right to lodge a complaint with the ICO.

g) Where the personal data is not collected from the data subject, any available information as to their source.

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

i) Where personal data is transferred outside the UK, details of the appropriate safeguards to protect the personal data.

2.3 We shall also, unless there is an exemption (see paragraph nine below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex,

or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

2.4 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if it contains the personal data of other data subjects. If it does, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

2.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request. However, we are not permitted to charge a general fee for responding to an SAR.

2.6 If we are not going to respond to the SAR, we shall inform the data subject of the reason(s) and of the possibility of lodging a complaint with the ICO.

3. Responding to requests to rectify personal data

3.1 Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding their data. Where such a request is made, we shall, unless there is an exemption (see paragraph nine below), rectify the personal data without undue delay.

3.2 We shall also communicate the rectification of the personal data to each recipient to whom the personal data has been disclosed (for example, our third-party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4. Responding to requests for the erasure of personal data

4.1 Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see paragraph nine below), erase the personal data without undue delay if:

a) The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

b) The data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data was processed and there is no other legal basis for the processing.

c) The data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest, or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we can either show compelling, legitimate grounds for the processing which

override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims.

d) The data subject objects to the processing of their personal data for direct marketing purposes.

e) The personal data has been unlawfully processed.

f) The personal data has to be erased for compliance with a legal obligation to which we are subject.

g) The personal data has been collected in relation to the offer of e-commerce or other online services.

4.2 When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see paragraph 4.5 and paragraph nine below), take the following steps:

a) Log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met).

b) Confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this.

c) Search databases, systems, applications and other places where the personal data which is the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

d) Where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, that personal data.

e) Communicate the erasure of the personal data to each recipient to whom the personal data has been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request (see paragraph 4.5 below).

4.4 If we are not going to respond to the request, we shall inform the data subject of the reasons why and of the possibility of lodging a complaint with the ICO.

4.5 In addition to the exemptions in paragraph nine below, we can also refuse to erase the personal data to the extent processing is necessary:

a) For exercising the right of freedom of expression and information

b) For compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us

c) For reasons of public interest in the area of public health

d) For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing, or

e) For the establishment, exercise or defence of legal claims.

5. Responding to requests to restrict the processing of personal data

5.1 Data subjects have the right, unless there is an exemption (see paragraph nine below), to restrict the processing of their personal data if:

a) The data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data

b) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of its use instead

c) We no longer need the personal data for the purposes we collected it, but it is required by the data subject for the establishment, exercise or defence of legal claims, and

d) The data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

5.2 Where processing has been restricted, we shall only process the personal data (excluding storing it):

a) With the data subject's consent

b) For the establishment, exercise or defence of legal claims

c) For the protection of the rights of another person, or

d) For reasons of important public interest.

5.3 Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

5.4 We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data has been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

6. Responding to requests for the portability of personal data

6.1 Data subjects have the right, in certain circumstances, to receive their personal data provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, we shall, unless there is an exemption (see paragraph nine below), provide the personal data without undue delay if:

a) The legal basis for the processing of the personal data is consent or pursuant to a contract, and

b) Our processing of that data is automated.

6.2 When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps:

a) Log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met).

b) Confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity.

c) Search databases, systems, applications and other places where the personal data which is the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

6.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

6.4 If we are not going to respond to the request, we shall inform the data subject of the reasons and of the possibility of lodging a complaint with the ICO.

7. Responding to objections to the processing of personal data

7.1 Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either:

a. Can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or

b. Are processing the personal data for the establishment, exercise or defence of legal claims.

7.2 Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

7.3 Where such an objection is made, we shall, unless there is an exemption (see paragraph nine below), no longer process a data subject's personal data.

7.4 Where personal data is processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

8. Responding to requests not to be subject to automated decision-making

8.1 Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see paragraph nine below), no longer make such a decision unless it:

a. Is necessary for entering into or the performance of a contract between us and the data subject

b. Is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, or

c. Is based on the data subject's explicit consent.

8.2 If the decision falls within paragraph 8.1(a) or paragraph 8.1(c), we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

9. Exemptions

9.1 Before responding to any request, we shall check whether there are any exemptions that apply to the personal data that is the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:

a) National security

b) Defence

c) Public security

d) The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

e) Other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security

f) The protection of judicial independence and judicial proceedings

g) The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions

h) A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in paragraph 9.1(a) and paragraph 9.1(g) above

i) The protection of the data subject or the rights and freedoms of others, or

j) The enforcement of civil law claims.

9. Schedule 3 – Data breach response protocol

1. Governance

1.1 Who is responsible for what and appropriate overall management of breach response:

- Data Privacy Manager – coordination of breach response and all elements feeding into response, including advice on compliance with UK GDPR requirements.
- Heads of departments and managing directors – input into response relating to area of expertise/involvement with the breach, as directed by the DPM.
- IT Director – must be involved in any aspects of the breach that relate to IT issues.
- HR Director – must be involved in any aspects of the breach that relate to employees or employee data.
- Communications team – must be involved in any formal internal or external communications being distributed, to be contacted as soon as possible after identifying that such communications will be necessary.
- Chief Executive Officer (CEO), Chief Financial Officer (CFO) and Group General Counsel – to be informed of the breach initially and then updated at regular intervals, responsible for decision-making (if required) in relation to elements of breach response.
- Board of Directors – to be informed of the breach initially and then to receive report following the breach detailing the incident and issues raised/lessons learned.

2. Detection

All employees are required to be vigilant in identifying potential data breaches. On identification of a potential breach, notification should be as per section three below.

3. Escalation procedure

a) On discovery of a potential data breach, an employee shall notify the DPM immediately.

b) The DPM shall then notify:

- IT Director (if relating to an IT breach)
- HR Director (if relating to employee or employee data)
- Other department heads or managing directors where the breach directly and specifically affects them or their department/subsidiary
- CEO, CFO and General Counsel

c) The above notified persons shall meet or conduct a conference call within 24 hours of the breach being notified to the DPM, to discuss:

- Whether this is a personal data breach and if so whether it requires notification to the ICO (note: breaches not notified should be recorded by the DPM)
- Initial required actions
- Initial position regarding communications (see section four below for further details)
- Any additional internal stakeholders that should be informed and/or involved in the breach response
- The method and timing of initial notification to the Board of Directors
- Roles and responsibilities
- In all cases, the parties shall take into account the considerations set out in sections four and five of this schedule, below

d) Within a further 24 hours of the meeting/call referred to in (c) above, the same parties shall meet or conduct a further conference call to discuss any updates to the above issues, and shall continue to meet in this pattern every 24 hours unless agreed otherwise (and/or it is agreed that a smaller subset of the parties should continue to meet).

e) The same parties (or a smaller subset of them, as agreed) shall seek to provide a full report to the Board regarding the breach within four weeks of the breach and/or by the next occurring group board meeting, whichever is longer.

4. Communications

4.1 Communications generally

As stated under ‘governance,’ above, all communications, whether internal or external, should involve the communications team, to ensure coordination of response and consistent messaging throughout the group.

4.2 Timeline and process

(a) Notification to the supervisory authority

A data controller must notify a data breach to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it. A data controller is deemed to become aware of a data breach when the controller has "a reasonable degree of certainty" that the incident affects personal data. Therefore, the moment when breach awareness develops (in the form of a reasonable degree of certainty that the breach has occurred) marks the start of the 72-hour deadline to notify the ICO. In practice, the threshold of a reasonable degree of certainty is not always clear-cut and will be a call to be made by the DPM. This may be complicated if the breach has occurred in relation to one of our data processors, not by the group itself, and again should be referred immediately to the DPM for handling.

The following information should be included in a breach notification to the ICO:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

Due to the potential complexities of personal data breaches, it is likely in many situations that we may not have all the necessary information within 72 hours of when we become aware of the breach. Therefore, it is possible to provide this information in phases, provided further information is provided to the ICO without undue further delay. In practice, the initial notification to the ICO may be very high level within the initial 72-hour period, followed by more detailed information when the full nature and extent of the breach has been identified.

(b) Notification to individuals

There is no set deadline for notifications to individuals. However, this must be done without undue delay. The exact timeline will depend on the circumstances. For example, the need to mitigate an immediate risk of damage would call for immediate communication, whereas the need to implement appropriate measures against continuing or similar personal data breaches, or to ensure that the full extent of the breach is understood before notifying employees, may justify more time for communication.

Guidance suggests that normally data subjects will be notified after the ICO, and following advice from that authority, but recognises that this will not always be the case, and importantly, that notifying the ICO will not serve as a justification for failure to communicate to data subjects. In other words, it is prudent not to wait for advice from the ICO if data subjects are plainly at risk in the meantime. Communications to the ICO shall clearly what approach is going to be adopted regarding data subject notification and invite challenge.

The following information should be included in a breach notification to individuals:

- The name and contact details of the DPM and/or other relevant contact point where more information can be obtained
- A description of the likely consequences of the personal data breach, and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

In practice, the ICO may assist us in identifying what information should be communicated to individuals, depending on the timing of notification to the ICO and to the individuals affected. Dedicated messages to individuals about data breaches should be made (not "buried" in other communications). Press releases or general media statements are unlikely to be seen as effective notification unless there is no other means of contacting the individuals. We will also communicate to affected individuals anything which the individuals can do themselves to mitigate the potential impacts of the breach (such as password changes, credit monitoring).

(c) Notification to law enforcement

In the majority of cases, where a breach has been due to criminal activity, notifying the relevant law enforcement agency of the breach (usually the Action Fraud team, or other relevant law enforcement agency relating to cyber crime/fraud, where relevant) will be carried out quickly and routinely. Only where that notification would cause additional security or other concerns will reporting be delayed, at the determination of the DPM in consultation with others.

5. Investigation and recovery/remediation

The parameters of the investigation will be set during the discussions between the parties pursuant to section three of this schedule above. The following aspects of the outcome of the investigation should be taken into account:

- *Requirements for information:* The level of detail required for any notifications and communications with data subjects and the ICO (and others as applicable).
- *Engagement of experts:* Whether it will be necessary to engage any professional advisers (IT, legal, risk, insurance etc) to assist with assessment and response of the breach.
- *Reputational risk:* Serious consideration will always need to be given to when we should notify a breach. Delaying the provision of information which data subjects (especially consumer customers) would see as relevant and important, risks increasing reputational damage, and this should be balanced against the need to ensure that any communication is accurate and thorough.
- *Remediation:* Conversely, in practical terms it may be appropriate to make breach notifications to regulators and data subjects when it is possible to say that the breach has been dealt with and shut down, or at least that there is a firm plan to do so. This will influence the notification and communication strategy throughout, as it is one of the first questions which supervisory authorities and interested data subjects will ask. It is therefore a key priority to focus on incident response.
- *Enabling downstream mitigation:* Notifying data subjects allows them the opportunity to do something about the risk to them, especially in circumstances where fraud may follow as a consequence of the breach. This has the practical

effect of limiting breach impact and minimising the risks associated with potential fines or claims for failure to properly adopt appropriate security measures.

- *Privilege*: Investigations into what has happened in a breach situation, and especially why or how it has happened, will probably throw up conclusions in raw form which it would not be attractive to disclose to regulators or in litigation. While there are clear limits to whether outside investigations by technical providers will qualify for privilege, it must be carefully considered as to how best to maximise the potential for privilege to apply and make appropriate arrangements accordingly.
- *Evidence preservation:* Evidence gathered in breach investigation is likely to be relevant in multiple respects. It may need to be used to defend claims associated with failure to implement appropriate security measures, or around handling of the breach. It may be used in proactive civil litigation strategies against threat actors themselves, or it may be important for criminal prosecution of threat actors. It should therefore be gathered in a proper, forensic way and with appropriate "chain of custody" records. This is especially delicate in the case of cyber investigations, and it should be noted that this requirement may conflict with remediation.
- *Proactive remedies against the threat actor or subsequent recipients:* It may be possible to trace threat actors or to use legal methods to seek to stop a cyberattack, such as third-party disclosure orders, or takedown requests/injunctive action to disable assets being used in an attack. Equally, it may be possible to manage the impact by actions against third parties to prevent further distribution/use/publication of material obtained in a data breach.
- *CIRT involvement*: Involving a national cyber incident response team (CIRT) (in the UK, the NCSC) has the benefit of allowing a controller to say that their handling of the breach has pulled advice from the most authoritative of resources. CIRTs may be able to share specific intelligence on threat actors which is not generally available and may assist in breach response.
- *HR considerations*: Employee rights need to be considered. In particular, a data breach response may require the implementation of much more invasive monitoring of employee activity than is normally the case. Careful consideration must be given to the data protection aspects of that monitoring, as well as to any broader employee rights considerations. Further, more complex, considerations may arise if there is suspicion of active insider involvement in the breach in question.
- *Paying ransoms*: Ransomware or other extortion mechanisms have ethical considerations for organisations and may raise legal considerations. In the UK, it is unlikely that the payment of a ransom of itself would constitute an offence or give rise to liability, but it is a decision on which we will wish to make an ethical position. It also affects breach notification strategy, as we may not wish to state publicly that a breach was remediated by the payment of a ransom. There may also be a question as to whether insurance coverage (if in place at all) will cover any ransom payment.

10. Appendix 1 – Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits ADM (unless certain conditions are met) but not automated processing.

Automated processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing, as are many uses of artificial intelligence (AI) where they involve the processing of personal data.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the UK GDPR. The Group is the Data Controller of all Personal Data relating to our Group Personnel and Personal Data used in our business for our own commercial and other relevant and justified purposes.

Data subject: a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the processing of personal data.

Data Privacy Manager: Amy Stanbridge, General Counsel and Company Secretary, or a replacement appointed from time to time. Because a mandatory data privacy manager does not need to be appointed by the group, this is a voluntary appointment of a person responsible for advising on and creating all documents relating to the UK GDPR and all issues arising from compliance with it.

Explicit consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal data is subject to the legal safeguards specified in the UK GDPR.

Group personnel/staff: all employees, workers, contractors, agency workers, directors, members and others who work within or for the group.

ICO: the Information Commissioner’s Office

Personal data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Privacy by design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy notices/fair processing notices: separate notices setting out information that may be provided to data subjects when the group collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing or process: any activity that involves the use of personal 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 transmitting or transferring personal data to third parties.

Pseudonymisation or pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related policies: the group's policies, operating procedures or processes related to this policy and designed to protect personal data, including:

- Information systems and security policy
- Document management policy
- Social media policy

Special categories of personal data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.