MM&K Limited
Data Protection Policy

April 2024

1. Introduction

This Policy sets out the obligations of MM & K Limited, a company registered in England under number 1983794, whose registered office is at 6th Floor, Kings House, 9/10 Haymarket, LONDON, SW1Y 4BP ("the Company") regarding data protection and the rights of its Clients and business contacts ("data subjects") in respect of their personal data under Data Protection Law. "Data Protection Law" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to Staff, Clients, Suppliers and Business Contacts used in our business for our commercial purposes;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom the Company holds personal data;
"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"personal data"	means any information relating to a data subject

	who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. Scope

3.1 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

3.2 The Company's Data Protection Officer is Joanne Fegan joanne.fegan@mm-k.com. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

3.3 All Directors are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.4 Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and/or process personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing.

4. The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

4.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

4.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

4.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

4.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

4.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures

required by the UK GDPR in order to safeguard the rights and freedoms of the data subject.

4.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

The UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

5.1 The right to be informed (Part 14).

5.2 The right of access (Part 15);

5.3 The right to rectification (Part 16);

5.4 The right to erasure (also known as the 'right to be forgotten') (Part 17);

5.5 The right to restrict processing (Part 18);

5.6 The right to data portability (Part 19);

5.7 The right to object (Part 20); and

5.8 Rights with respect to automated decision-making and profiling (Parts 21 and 22).

6. Lawful, Fair, and Transparent Data Processing

6.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a) The data subject has given consent to the processing of their personal data for one or more specific purposes;

b) The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

c) The processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) The processing is necessary to protect the vital interests of the data subject or of another natural person;

e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are

overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7. Specified, Explicit, and Legitimate Purposes

7.1 The Company collects and processes the personal data set out in Part 20 of this Policy. This includes:

a) Personal data collected directly from data subjects; and

b) Personal data obtained from third parties.

7.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 20 of this Policy (or for other purposes expressly permitted by the UK GDPR).

7.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 14 for more information on keeping data subjects informed.

8. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

9. Accuracy of Data and Keeping Data Up-to-Date

9.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 16, below.

9.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

10. Data Retention

10.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

10.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

10.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

11. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 20 to 29 of this Policy.

12. Accountability and Record-Keeping

12.1 The Company's Data Protection Officer is Joanne Fegan joanne.fegan@mm-k.com.

12.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

12.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

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

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

d) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

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

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

13. Data Protection Impact Assessments

13.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

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

a) The type(s) of personal data that will be collected, held, and processed;

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

c) The Company's objectives;

d) How personal data is to be used;

e) The parties (internal and/or external) who are to be consulted;

f) The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) Risks posed to data subjects;

h) Risks posed both within and to the Company; and

i) Proposed measures to minimise and handle identified risks.

14. Keeping Data Subjects Informed

14.1 The Company shall provide the information set out in Part 14.2 to every data subject:

a) Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i. if the personal data is used to communicate with the data subject, when the first communication is made; or

ii. if the personal data is to be transferred to another party, before that transfer is made; or

iii. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

14.2 The following information shall be provided:

a) Details of the Company including, but not limited to, the identity of its Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 20 of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place;

g) Details of data retention;

h) Details of the data subject's rights under the UK GDPR;

i) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

l) Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

15. Data Subject Access

15.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

15.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at joanne.fegan@mm-k.com

15.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

15.4 All SARs received shall be handled by the Company's Data Protection Officer.

15.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. Rectification of Personal Data

16.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

16.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

16.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

17. Erasure of Personal Data

17.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 19 of this Policy for further details concerning the right to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

17.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

18. Restriction of Personal Data Processing

18.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

18.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

19. Objections to Personal Data Processing

19.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling.

19.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate

grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

19.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

20. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
1	Work email address	To carry out our services contracted by You, and provide information regarding our other services and marketing initiatives
2	Job title	To carry out our services contracted by You, and provide information regarding our other services and marketing initiatives
3	Telephone numbers provided by you	In order to contact you directly in order to carry out our services contracted by You.
4	Company Name and Address	In order to send mail directly to you in order to carry out our services contracted by You.
5	Personal email address	If You provide a personal email address for correspondence, We will use this email to contact you in order to carry out our contracted services to You and may also use this email address for marketing purposes.

21. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

21.1 All emails containing personal data must be password protected;

21.2 All emails containing personal data must be marked "confidential";

21.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

21.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

21.5 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

21.6 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

21.7 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient where possible; and

21.8 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

22. Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

22.1 All electronic copies of personal data should be stored securely using passwords;

22.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

22.3 All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted;

22.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of Joanne Fegan Manging Partner Joanne Fegan joanne.fegan@mm-k.com and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

22.5 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

23. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

24. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

24.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access

to any personal data that they do not already have access to, such access should be formally requested from Joanne Fegan joanne.fegan@mm-k.com;

24.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Joanne Fegan joanne.fegan@mm-k.com;

24.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

24.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

24.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Operations Director to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

25. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

25.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;

25.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

25.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible , unless there are valid technical reasons not to do so; and

25.4 No software may be installed on any Company-owned computer or device without the prior approval of the Operations Director.

26. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

26.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the UK GDPR and under this Policy, and shall be provided with a copy of this Policy;

26.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry

out their assigned duties correctly shall have access to personal data held by the Company;

26.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

26.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

26.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

26.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

26.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

26.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

26.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract;

26.10 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the UK GDPR; and

26.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27. Transferring Personal Data Outside the UK

27.1 The Company may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

27.2 Personal data may only be transferred to a country outside the UK if one of the following applies:

a) The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.

b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes

those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.

c) The transfer is made with the informed and explicit consent of the relevant data subject(s).

d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

28. Data Breach Notification

28.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

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

28.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

28.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

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

29. Implementation of Policy

This Policy shall be deemed effective as of 1 April 2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.