



DATA PROTECTION POLICY

FOR:

KPH GROUP

**KPH ENVIRONMENTAL SERVICES LTD
AND KPH DECONSTRUCTION LTD**

AS REQUIRED BY:

GENERAL DATA PROTECTION REGULATIONS

AND

DATA PROTECTION ACT 2018

OFFICE COPY (CONTROLLED DOCUMENT)

DOCUMENT TITLE:	DATA PROTECTION POLICY
DOCUMENT NO:	KpH Data Protection Policy
DATE:	01 AUGUST 2022
ISSUE NO:	5

AMENDMENT RECORD:

Issue No.	Summary of Change	Date	Author	Initialled	Reviewed by
01	First Issue	25/05/2018	Amy Hathaway	AH	LW PB MW SD KP
02	Annual Review	31/08/2019	Steve Dellaway	SD	LW MW KP
03	GDPR Process Additions	21/01/2020	Amy Hathaway	AH	LW SD
04	Annual Review – Legislative Changes	03/08/2021	Lyndsey West	LW	MW KP SD
05	Annual Review	01/08/2022	Lyndsey West	LW	MW
06					
07					
08					
09					
10					
11					
12					

CONTENTS

1. INTRODUCTION	4
2. DATA PROTECTION PRINCIPLES	4
3. LAWFUL FAIR AND TRANSPARENT DATA PROCESSING	5
4. PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES	5
5. ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING	5
6. ACCURACY OF DATA AND KEEPING DATA UP TO DATE	5
7. TIMELY PROCESSING	6
8. SECURE PROCESSING	6
9. ACCOUNTABILITY	6
10. PRIVACY IMPACT ASSESSMENT	6
11. THE RIGHTS OF DATA SUBJECTS	7
12. KEEPING DATA SUBJECTS INFORMED	7
13. DATA SUBJECT ACCESS REQUEST (SAR)	8
14. RECTIFICATION OF PERSONAL DATA	9
15. ERASURE OF PERSONAL DATA (“REQUEST TO BE FORGOTTEN”)	9
16. RESTRICTION OF PERSONAL DATA PROCESSING	10
17. DATA PORTABILITY	10
18. OBJECTIONS TO PERSONAL DATA PROCESSING	10
19. AUTOMATED DECISION-MAKING	11
20. PROFILING	11
21. PERSONAL DATA	12
22. DATA PROTECTION MEASURES	12
23. ORGANISATIONAL MEASURES	14
24. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA	14
25. DATA BREACH NOTIFICATION	15
26. IMPLEMENTATION OF POLICY	16
APPENDIX 1 - DEFINITIONS	17
APPENDIX 2 – WORKFLOW PROCESS: SUBJECT ACCESS REQUEST (SAR)	20
APPENDIX 3 – WORKFLOW PROCESS: REQUEST TO BE FORGOTTEN	21
APPENDIX 4 – WORKFLOW PROCESS: DATA BREACH	22

1. INTRODUCTION

- 1.1 This Policy sets out the obligations of KpH Group (“the Company”) regarding data protection and the rights of direct employees, agency staff, customers, sub-contractors, business contacts, members of the public (“data subjects”) in respect of their personal data under the UK-GDPR and 2018 Data Protection Regulation (“the Regulation”).
- 1.2 The Regulation defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- 1.3 This Policy sets out the procedures that are to be followed when dealing with 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.
- 1.4 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.

2. DATA PROTECTION PRINCIPLES

- 2.1 This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:
 - a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
 - b) 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;
 - c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
 - d) 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 they are processed, is erased or rectified without delay;
 - e) 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 Regulation in order to safeguard the rights and freedoms of the data subject;
 - f) 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.

3. LAWFUL FAIR AND TRANSPARENT DATA PROCESSING

- 3.1 The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation 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 his or her personal data for one or more specific purposes;
 - b) 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;
 - c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;
 - d) processing is necessary **to protect the vital interests of the data subject** or of another natural person;
 - e) 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 controller;
 - f) processing is necessary for the purposes of the **legitimate interests** pursued by the 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.

4. PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

- 4.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, contact details or training records from a Sub-Contractor).
- 4.2 The Company only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING

- 5.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. ACCURACY OF DATA AND KEEPING DATA UP TO DATE

- 6.1 The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. TIMELY PROCESSING

- 7.1 The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. SECURE PROCESSING

- 8.1 The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. ACCOUNTABILITY

- 9.1 The Company's Data Protection Manager is Steve Dellaway and his contact details are Telephone: 01883 346604 and Email: steve.dellaway@kph.co.uk.
- 9.2 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 Manager, and any applicable third-party data controllers.
 - b) The purposes for which the Company 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 (and categories) of any third parties that will receive personal data from the Company.
 - e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.
 - f) Details of how long personal data will be retained by the Company.
 - g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. PRIVACY IMPACT ASSESSMENT

- 10.1 The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall address the following areas of importance:
- a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data.
 - b) Details of the legitimate interests being pursued by the Company.
 - c) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

- d) An assessment of the risks posed to individual data subjects.
- e) Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. THE RIGHTS OF DATA SUBJECTS

11.1 The Regulation sets out the following rights applicable to data subjects:

- a) The right to be informed.
- b) The right of access.
- c) The right to rectification.
- d) The right to erasure (also known as the 'right to be forgotten').
- e) The right to restrict processing.
- f) The right to data portability.
- g) The right to object.
- h) Rights with respect to automated decision-making and profiling.

12. KEEPING DATA SUBJECTS INFORMED

12.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:

- a) Details of the Company including, but not limited to, the identity it's Data Protection Manager.
- b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 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 European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers).
- g) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined).
- h) Details of the data subject's rights under the Regulation.

- 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 Regulation).
 - 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.
 - l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.
- 12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:
- 12.3 Where the personal data is obtained from the data subject directly, at the time of collection;
- 12.4 Where the personal data is not obtained from the data subject directly (i.e. from another party):
- a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
 - b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
 - c) In any event, not more than one month after the time at which the Company obtains the personal data.

13. DATA SUBJECT ACCESS REQUEST (SAR)

- 13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within 28 days of receipt (this can be extended by up to 56 days in the case of complex and/or numerous requests, and in such cases, the data subject must be informed of the need for the extension).
- 13.2 All subject access requests received must be forwarded to Steve Dellaway, the Company's Data Protection Manager (steve.dellaway@kph.co.uk), to process the request and record the outcome on the **Access Log**.
- 13.3 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.

13.4 Please see **Appendix B** for a Workflow Process Diagram on Subject Access Requests (SAR).

14. RECTIFICATION OF PERSONAL DATA

- 14.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
- 14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. ERASURE OF PERSONAL DATA ("REQUEST TO BE FORGOTTEN")

- 15.1 Data subjects may request that the Company erases the personal data it holds about them (otherwise known as a "request to be forgotten") in the following circumstances:
- a) It is no longer necessary for the Company to hold that personal data with respect to the purpose 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 18 of this Policy for further details concerning data subjects' rights 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.
- 15.2 The Data Protection Manager must be notified of the request so that arrangements can be made for the request to be processed within the appropriate timeframe and recorded on the Request to be Forgotten Log.
- 15.3 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 28 days of receipt of the data subject's request (this can be extended by up to 56 days in the case of complex requests; however, in such cases, the data subject must be informed of the need for the extension).
- 15.4 In the event that any personal data that is to be erased (in response to a data subject 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).
- 15.5 Please see **Appendix C** for a Workflow Process Diagram on Requests to be Forgotten.

16. RESTRICTION OF PERSONAL DATA PROCESSING

- 16.1 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 pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
- 16.2 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).

17. DATA PORTABILITY

- 17.1 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers e.g. other organisations).
- 17.2 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format[s]:
- a) electronic;
 - b) as requested.
- 17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.
- 17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. OBJECTIONS TO PERSONAL DATA PROCESSING

- 18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].
- 18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
- 18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.
- 18.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. AUTOMATED DECISION-MAKING

19.1 In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

19.2 The right described in Part 19.1 does not apply in the following circumstances:

- a) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject.
- b) The decision is authorised by law.
- c) The data subject has given their explicit consent.

20. PROFILING

20.1 Where the Company uses personal data for profiling purposes, the following shall apply:

- a) Clear information explaining the profiling will be provided, including its significance and the likely consequences.
- b) Appropriate mathematical or statistical procedures will be used.
- c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
- d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. PERSONAL DATA

21.1 The following personal data may be collected, held, and processed by the Company:

Data Category	Reason the Data Collected, Held and Processed
Marketing	Information is collected to keep current and prospective clients up to date with our services, work and achievements.
Accounts	Information is collected to process payroll and financial transactions.
Health and Safety	Information is collected and shared as required to maintain regulation Health and Safety standards and practices.
Human Resources	Information is collected and processed to manage staff contracts and welfare.
Operations	Information is collected, shared and distributed to maintain health and safety standards and carry out our services as contracted.
Quality	Information is processed to meet Quality standards, maintain health and safety practices and evidence compliance with industry regulations.
Tendering	Information is presented to potential clients, providing evidence of our standards and experience, to win work.
Yard	Information is collected and processed to manage the assets and equipment movement in the yard and maintain appropriate Health and Safety standards.

21.2 Please see our **Document Longevity Retention Matrix** for a comprehensive list of personal data and full descriptive details.

22. DATA PROTECTION MEASURES

22.1 The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) All emails containing personal data must be encrypted using Office365 mail encryption services.
- b) Where 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. Hardcopies should be shredded, and electronic copies should be deleted securely using S Delete or Windows Cipher.
- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
- e) 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.
- f) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent in the post by recorded delivery, marked private and confidential.

- g) 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 Steve Dellaway, Data Protection Manager.
- h) 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.
- i) 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 Data Protection Manager, Steve Dellaway (Email: steve.dellaway@kph.co.uk).
- j) 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.
- k) 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.
- l) 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 Data Protection Manager, Steve Dellaway (Email: steve.dellaway@kph.co.uk) 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].
- m) 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 Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken.
- n) All personal data stored electronically should be backed up daily onsite and offsite. All backups should be encrypted using AES encryption.
- o) All electronic copies of personal data should be stored securely using passwords and AES data encryption.
- p) All passwords used to protect personal data must comply with the company's **Information Security Policy**.
- q) 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.
- r) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Business Development and Quality Co-Ordinator to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked as and when required.

23. ORGANISATIONAL MEASURES

- 23.1 The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
- a) 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 Regulation and under this Policy, and shall be provided with a copy of this Policy.
 - b) 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.
 - c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
 - d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.
 - e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
 - f) 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.
 - g) 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 Regulation and this Policy by contract.
 - h) 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 Regulation.
 - i) 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.

24. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

- 24.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
- 24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
- a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data.

- b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.
- c) The transfer is made with the informed consent of the relevant data subject(s).
- d) The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject).
- e) The transfer is necessary for important public interest reasons.
- f) The transfer is necessary for the conduct of legal claims.
- g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent.
- h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. DATA BREACH NOTIFICATION

- 25.1 All personal data breaches must be reported immediately to the Company's Data Protection Manager for investigation and recording on the Data Breach Log.
- 25.2 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 Manager must ensure that the Information Commissioner's Office (ICO) is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the Data Protection Manager must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 25.4 Please see **Appendix D** for a Workflow Process Diagram on Data Breaches.


25.5 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 Manager (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.

26. IMPLEMENTATION OF POLICY

26.1 This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Mr Kevin Potter
Position:	Managing Director
Date:	01/08/2022
Due for Review by:	31/07/2023
Signature:	

In case of any queries or questions in relation to this policy please contact us info@kph.co.uk.

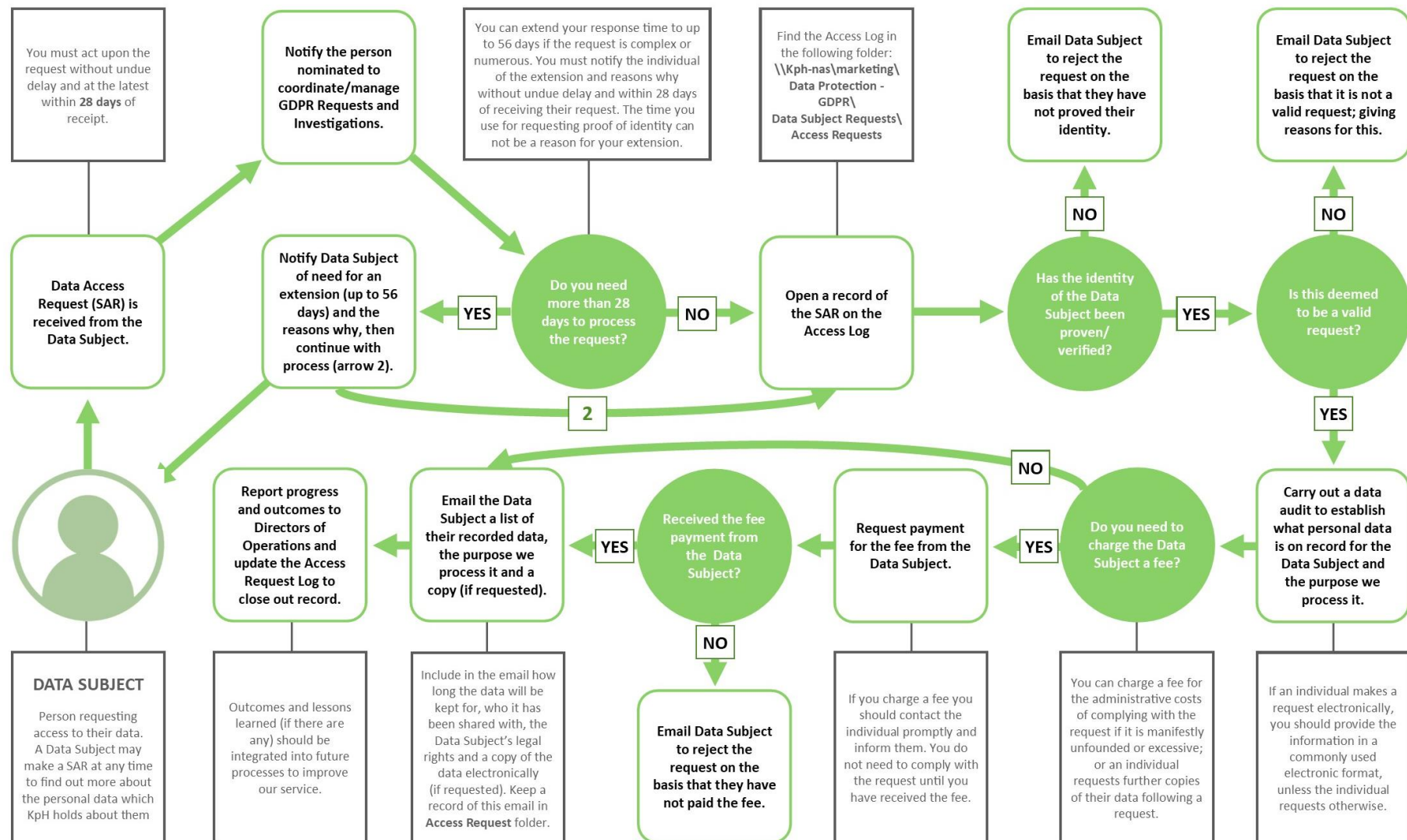
APPENDIX 1 - DEFINITIONS

- (1) **‘personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) **‘processing’** means any operation or set of operations which is performed on personal data or on 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;
- (3) **‘restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) **‘profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (5) **‘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 are not attributed to an identified or identifiable natural person;
- (6) **‘filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- (7) **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (8) **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- (9) **‘recipient’** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 L 119/33 Official Journal of the European Union EN framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- (10) **‘third party’** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- (11) **‘consent’** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

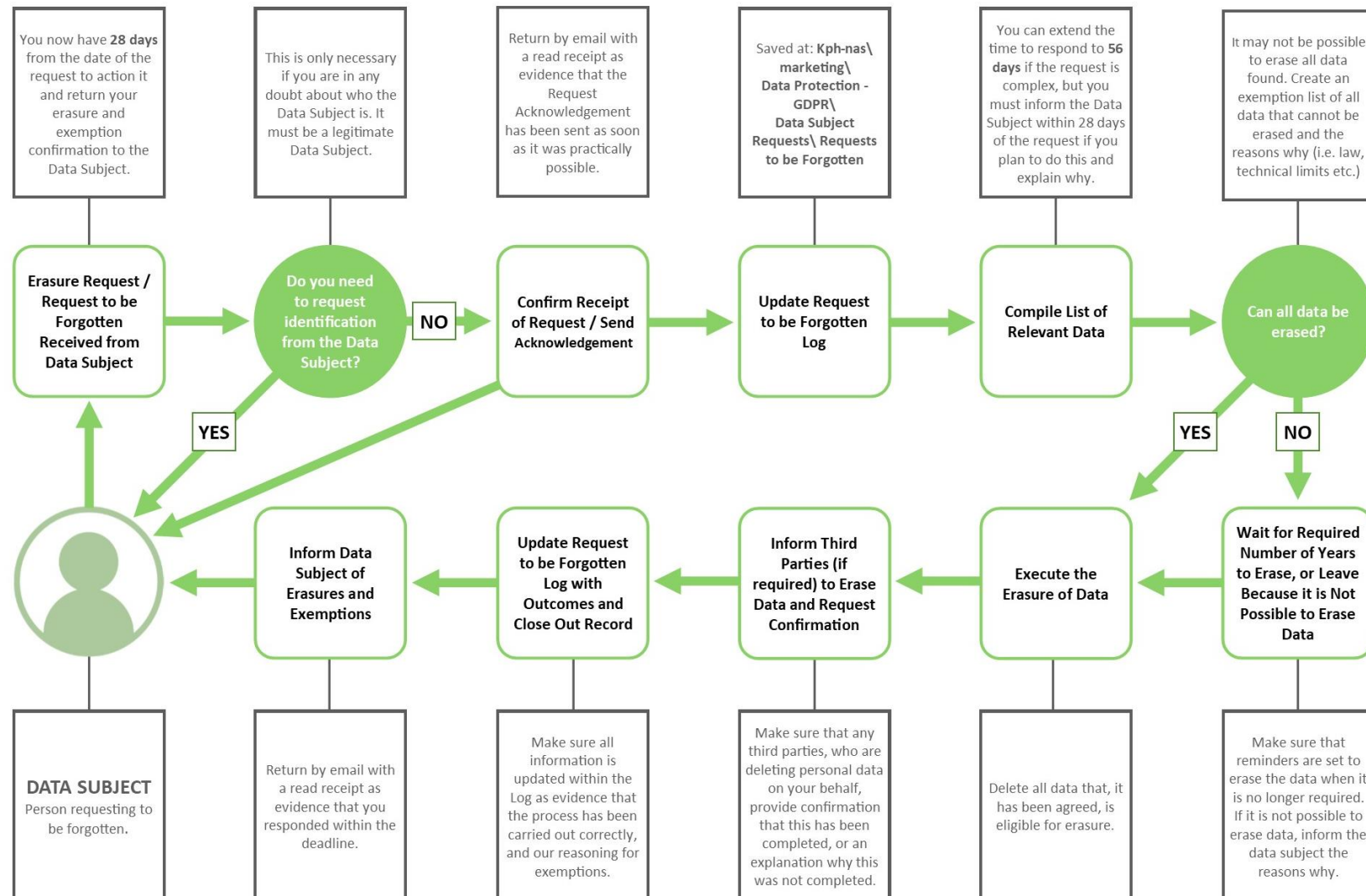
- (12) **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (13) **‘genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- (14) **‘biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (15) **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- (16) **‘main establishment’** means:
- a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
 - b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
- (17) **‘representative’** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- (18) **‘enterprise’** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- (19) **‘group of undertakings’** means a controlling undertaking and its controlled undertakings;
- (20) **‘binding corporate rules’** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- (21) **‘supervisory authority’** means an independent public authority which is established by a Member State pursuant to Article 51; 4.5.2016 L 119/34 Official Journal of the European Union EN;

- (22) **‘supervisory authority concerned’** means a supervisory authority which is concerned by the processing of personal data because:
- a) the controller or processor is established on the territory of the Member State of that supervisory authority;
 - b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
 - c) a complaint has been lodged with that supervisory authority;
- (23) **‘cross-border processing’** means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
- (24) **‘relevant and reasoned objection’** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- (25) **‘information society service’** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);
- (26) **‘international organisation’** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

APPENDIX 2 – WORKFLOW PROCESS: SUBJECT ACCESS REQUEST (SAR)



APPENDIX 3 – WORKFLOW PROCESS: REQUEST TO BE FORGOTTEN



APPENDIX 4 – WORKFLOW PROCESS: DATA BREACH

