

Data Protection Policy



Date published: May 2023

Department Responsible for Policy: Operations

Approving director: Managing Director

1. Introduction

This Policy sets out the obligations of SDN Enterprise Ltd, a company registered in England under number 05945050, whose registered office is at 4 Roberts Orchard Road, Barming, Maidstone, Kent, ME16 9HP ("SDN") regarding data protection and the rights of personal data ("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.

The GDPR 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.

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

2. Scope

- 2.1 SDN 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.
- 2.2 This policy should be read alongside the SDN GDPR Data Retention Policy.
- 2.3 All SDN Managers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of SDN comply with this Policy and, where applicable, must implement such practices, processes, controls, and training

as are reasonably necessary to ensure such compliance.

2.4 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:

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

2.4.2 if consent is being relied upon to collect, hold, and/or process personal data.

2.4.3 if there is any uncertainty relating to the retention period for any type(s) of personal data.

2.4.4 if any new or amended privacy notices or similar privacy-related documentation are required.

2.4.5 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).

2.4.6 if a personal data breach (suspected or actual) has occurred.

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

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

2.4.9 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.

2.4.10 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.

2.4.11 when personal data is to be used for purposes different to those for which it was originally collected.

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

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

3. 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:

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

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.

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

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.

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.

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.

4. 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):

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability

- The right to object; and
- Rights with respect to automated decision-making and profiling.

5. Lawful, Fair, and Transparent Data Processing

- 5.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:
- 5.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes.
 - 5.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract.
 - 5.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject.
 - 5.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person.
 - 5.1.5 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
 - 5.1.6 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.
- 5.2 If the personal data in question is special category personal data (also known as “sensitive personal data”), at least one of the following conditions must be met:
- 5.2.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so).
 - 5.2.2 the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides

for appropriate safeguards for the fundamental rights and interests of the data subject);

- 5.2.3 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- 5.2.4 the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- 5.2.5 the processing relates to personal data which is manifestly made public by the data subject.
- 5.2.6 the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.
- 5.2.7 the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- 5.2.8 the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;
- 5.2.9 the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- 5.2.10 the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19

of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6. Consent

6.1 If consent is relied upon as the lawful basis for collecting, holding and/or processing personal data, the following shall apply:

6.1.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

6.1.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

6.1.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

6.1.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

6.1.5 If special category personal data is processed, SDN shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

6.1.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that SDN can demonstrate its compliance with consent requirements.

7. Specified, Explicit, and Legitimate Purposes

7.1 SDN collects and processes the personal data set out in Part 21 of this Policy. This

includes:

- 7.1.1 Personal data collected directly from data subjects. AND
- 7.1.2 Personal data obtained from third parties.
- 7.2 SDN only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by Data Protection Law).
- 7.3 Data subjects are kept informed always of the purpose or purposes for which SDN uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

8. Adequate, Relevant, and Limited Data Processing

- 8.1 SDN 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) as under Part 8.
- 8.2 Employees, agents, contractors, or other parties working on behalf of SDN may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected. Personal data held by SDN cannot be processed for any unrelated reasons.

9. Accuracy of Data and Keeping Data Up to Date

- 9.1 SDN 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 14, 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 SDN 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 SDN's approach to data retention, including retention periods for specific personal data types held by SDN, please refer to our Data Retention Policy.

11. Secure Processing

- 11.1 SDN 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 22 to 27 of this Policy.
- 11.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
- 11.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:
- 11.3.1 only those with a genuine need to access and use personal data and who are authorised to do so may access and use it.
 - 11.3.2 personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
 - 11.3.3 authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

12. Accountability and Record-Keeping

- 12.1 The Head of Operations shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, SDN's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.
- 12.2 SDN shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- 12.2.1 The name and details of SDN, and any applicable third-party data processors.
 - 12.2.2 The purposes for which SDN collects, holds, and processes personal data.
 - 12.2.3 Details of the categories of personal data collected, held, and processed by SDN, and the categories of data subject to which that personal data relates.
 - 12.2.4 Details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards.

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

12.2.6 Detailed descriptions of all technical and organisational measures taken by SDN to ensure the security of personal data.

13. Data Protection Impact Assessments

13.1 SDN shall carry out a Data Protection Impact Assessment Screening for all new projects and/or new uses of personal data which involve the use of new technologies.

13.2 The screening process shall be overseen by the Head of Operations

13.3 SDN will always carry out a Data Protection Impact Assessment for processing that is likely to result in a high risk for individual.

13.4 Data Protection Impact Assessments shall be overseen by the Head of Operations and shall address the following:

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

13.4.2 The purpose(s) for which personal data is to be used.

13.4.3 SDN's objectives.

13.4.4 How personal data is to be used.

13.4.5 The parties (internal and/or external) who are to be consulted.

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

13.4.7 Risks posed to data subjects.

13.4.8 Risks posed both within and to SDN; and

13.4.9 Proposed measures to minimise and handle identified risks.

14. Keeping Data Subjects Informed

14.1 SDN shall provide the information set out in Part 15.2 to every data subject:

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

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

- a) if the personal data is used to communicate with the data subject, when the first communication is made; or
- b) if the personal data is to be transferred to another party, before that transfer is made; or
- c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

14.1.3 Details of SDN.

14.1.4 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.

14.1.5 Where applicable, the legitimate interests upon which SDN is justifying its collection and processing of the personal data.

14.1.6 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.

14.1.7 Where the personal data is to be transferred to one or more third parties, details of those parties.

14.1.8 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 (see Part 28 of this Policy for further details);

14.1.9 Details of data retention.

14.1.10 Details of the data subject's rights under the UK GDPR.

14.1.11 Details of the data subject's right to withdraw their consent to SDN's processing of their personal data at any time.

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

14.1.13 where the personal data is not obtained directly from the data subject, details about the source of that personal data.

- 14.1.14 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
- 14.1.15 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 SDN holds about them, what it is doing with that personal data, and why. This request should be sent to hello@strategicdevelopmentnetwork.co.uk
- 15.2 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.
- 15.3 All SARs received shall be handled by SDN’s Operations Department.
- 15.4 SDN does not charge a fee for the handling of normal SARs. SDN 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 SDN to rectify any of their personal data that is inaccurate or incomplete.
- 16.2 SDN shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing SDN 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 If 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 SDN erases the personal data it holds about them in the following circumstances:

- 17.1.1 It is no longer necessary for SDN to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.
 - 17.1.2 The data subject wishes to withdraw their consent to SDN holding and processing their personal data.
 - 17.1.3 The data subject objects to SDN holding and processing their personal data (and there is no overriding legitimate interest to allow SDN to continue doing so)
 - 17.1.4 The personal data has been processed unlawfully.
 - 17.1.5 The personal data needs to be erased for SDN to comply with a legal obligation.
- 17.2 Unless SDN 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 SDN ceases processing the personal data it holds about them. If a data subject makes such a request, SDN 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 If 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 SDN processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

- 19.2 Where a data subject objects to SDN processing their personal data based on its legitimate interests, SDN shall cease such processing immediately, unless it can be demonstrated that SDN'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 SDN processing their personal data for direct marketing purposes, SDN shall cease such processing promptly.
- 19.4 Where a data subject objects to SDN processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "demonstrate grounds relating to his or her particular situation". SDN is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

20. Personal Data Collected, Held, and Processed

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

Type of Data	Purpose of Data
Personal	Marketing
Personal	Client information Supplier information Associate information
Special	Internal staff information

21. Data Security - Transferring Personal Data and Communications

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

21.2 Any data shared electronically will be only shared through a secure network.

- 21.3 All emails containing personal data must be marked “confidential”. (see annex 1 for further instructions)
- 21.4 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
- 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 transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail – Recorded or Sign For.
- 21.7 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

- 22.1 SDN shall ensure that the following measures are taken with respect to the storage of personal data:
- 22.2 All electronic copies of personal data should be stored securely using passwords and Microsoft data encryption.
- 22.3 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.
- 22.4 All personal data stored electronically should be backed up monthly with backups stored onsite. All backups should be encrypted.
- 22.5 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to SDN or otherwise without the formal approval 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
- 22.6 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 SDN where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to SDN that all suitable technical and organisational measures have been taken).

23. Data Security - Disposal

- 23.1 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 SDN's Data Retention Policy.

24. Data Security - Use of Personal Data

- 24.1 SDN shall ensure that the following measures are taken with respect to the use of personal data:
- 24.2 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of SDN requires access to any personal data that they do not already have access to, such access should be formally requested.
- 24.3 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of SDN or not, without authorisation.
- 24.4 Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.
- 24.5 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it; and
- 24.6 Where personal data held by SDN is used for marketing purposes, it shall be the responsibility of Head of Business Development 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

- 25.1 SDN shall ensure that the following measures are taken with respect to IT and information security:
- 25.2 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.
- 25.3 Under no circumstances should any passwords be written down or shared between

any employees, agents, contractors, or other parties working on behalf of SDN, 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.

- 25.4 All software (including, but not limited to, applications and operating systems) shall be kept up to date. SDN's staff shall be responsible for installing all security-related updates as soon as reasonably and practically possible; and
- 25.5 No software may be installed on any Company-owned computer or device without prior approval of a Manager or Director.

26. Organisational Measures

- 26.1 SDN shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
- 26.2 All employees, agents, contractors or other parties working on behalf of SDN shall be made fully aware of both their individual responsibilities and SDN's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;
- 26.3 Only employees, agents, sub-contractors, or other parties working on behalf of SDN 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 SDN;
- 26.4 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data.
- 26.5 All employees, agents, contractors, or other parties working on behalf of SDN handling personal data will be appropriately trained to do so.
- 26.6 All employees, agents, contractors, or other parties working on behalf of SDN handling personal data will be appropriately supervised.
- 26.7 All employees, agents, contractors, or other parties working on behalf of SDN 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;
- 26.8 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
- 26.9 All personal data held by SDN shall be reviewed periodically, as set out in SDN's Data Retention Policy.

- 26.10 The performance of those employees, agents, contractors, or other parties working on behalf of SDN handling personal data shall be regularly evaluated and reviewed.
- 26.11 All employees, agents, contractors, or other parties working on behalf of SDN handling personal data will be bound to do so in accordance with the principles of the Data Protection Law, GDPR and this Policy by contract.
- 26.12 All agents, contractors, or other parties working on behalf of SDN 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 SDN arising out of this Policy and Data Protection Law; and
- 26.13 Where any agent, contractor or other party working on behalf of SDN handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless SDN against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27. Transferring Personal Data to a Country Outside the EEA

- 27.1 SDN 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 to ensure that the level of protection given to data subjects is not compromised.
- 27.2 The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:
- 27.2.1 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.
- 27.2.2 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.
- 27.2.3 The transfer is made with the informed consent of the relevant data subject(s).
- 27.2.4 The transfer is necessary for the performance of a contract between the data subject and SDN (or for pre-contractual steps taken at the request of the data subject).
- 27.2.5 The transfer is necessary for important public interest reasons.

- 27.2.6 The transfer is necessary for the conduct of legal claims.
- 27.2.7 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; or
- 27.2.8 The transfer is made from a register that, under UK 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.
- 27.2.9 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 Head of Operations, who will be responsible for assessing the breach and determining if a supervisory authority needs to be notified. If an employee, agent, contractor, or other party working on behalf of SDN becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. All evidence relating to the personal data breach in question should be carefully retained and the Head of Operations notified immediately
- 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 Head of Operations 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 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained
- 28.4 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 Head of Operations must ensure that all affected data subjects are informed of the breach directly and without undue delay.

28.5 Data breach notifications shall include the following information:

28.5.1 The categories and approximate number of data subjects concerned.

28.5.2 The categories and approximate number of personal data records concerned.

28.5.3 The name and contact details of the Head of Operations (or other contact point where more information can be obtained).

28.5.4 The likely consequences of the breach.

28.5.5 Details of the measures taken, or proposed to be taken, by SDN 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 **May 2023**. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

30. Policy information

Revised: May 2023

Sources: SimplyDocs.co.uk

Review date: May 2024