Cavill Associates

public health consultancy

Data protection policy

Author: Dr Nick Cavil
Cavill Associates Ltd
Suite 13292,
PO Box 4336
Manchester
M61 0BW

t: +44 (0) 161 440 9127
nick@cavill.net
www.cavill.net

Dec 2021

1. Introduction

This Policy sets out the obligations of Cavill Associates Ltd (CA), regarding data protection and the rights of employees, associates, customers, suppliers ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").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 out CA'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 CA, its employees, associates, contractors, or other parties working on behalf of CA. CA 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. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. 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 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.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects

- 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
- Rights with respect to automated decision-making and profiling

4. Lawful, Fair, and Transparent Data Processing

- CA seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. In line with GDPR Progress Health Partnerships Ltd 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
  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.

2. If the personal data in question is "special category data" (also known as "sensitive personal data") for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation, at least one of the following conditions must be met:

a. The data subject has given their explicit consent to the processing of such data for one or more specified purposes
b. 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
c. 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
d. 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
e. The processing relates to personal data which is clearly made public by the data subject
f. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
g. 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
h. 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 GDPR
i. 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)
j. 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 GDPR 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.

5. Specified, Explicit, and Legitimate Purposes

- CA collects and processes personal data. This includes:
  a. Personal data collected directly from employees, associates, clients and suppliers and the general public as an element of specific commissioned programmes

b. Personal data obtained from third parties.

- CA only collects, processes, and holds personal data for the specific purposes of commissioned programmes (or for other purposes expressly permitted by the GDPR)
- Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

6. Adequate, Relevant, and Limited Data Processing

CA 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 and that is identified in company contracts.

7. Accuracy of Data and Keeping Data Up to Date

- CA 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 below.

- 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.

8. Data Retention

- CA 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. All persons and organisations will be informed f the length of time their data will be held before being destroyed.

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

- 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 identified contracts.

9. Secure Processing

CA 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.

10. Accountability and Record-Keeping

- CA's Data Protection Officer is Dr Nick Cavill, Cavill Associates Ltd's Managing Director. 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 GDPR and other applicable data protection legislation.
- CA shall keep 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
  f. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments

- The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.
- 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.

12. Keeping Data Subjects Informed

- CA shall provide the information 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:
  c. if the personal data is used to communicate with the data subject, when the first communication is made; or

d. if the personal data is to be transferred to another party, before that transfer is made; or
e. 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:
  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 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 28 of this Policy for further details);
  g. Details of data retention;
  h. Details of the data subject's rights under the 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 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.

13. Data Subject Access

- 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.
- Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer.
- 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.
- All SARs received shall be handled by the Company's Data Protection Officer.

14. Rectification of Personal Data

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

15. Erasure of Personal Data

- 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 18 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.
- 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.
- 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).

16. Restriction of Personal Data Processing

- 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.

- 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. Objections to Personal Data Processing

- Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling).
- 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.
- Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18. 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:

- All emails containing personal data will be treated as confidential
- All emails containing personal data must be marked "confidential"
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances
- 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
- 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
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
- 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".

19. Data Security – Storage

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

- All electronic copies of personal data should be stored securely using secured by passwords
- 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
- 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 GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken)
-

20. 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.

21. Data Security – Use of Personal Data

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

- 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 the Managing Director;
- 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 the Managing Director;
- 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;
- 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
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the DPO 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.

22. Data Security – IT Security

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

- 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.
- 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.
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date.
- No software may be installed on any Company-owned computer or device without the prior approval of the Managing Director.

23. Organisational Measures

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

- 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 GDPR and under this Policy, and shall be provided with a copy of this Policy
- 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
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised
- 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
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy
- 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

- 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 GDPR and this Policy by contract
- 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 GDPR; and
- 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. Data Breach Notification

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

25. Implementation of Policy

This Policy shall be deemed effective as of 25 Dec 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.