The Moredun Group Data Protection Policy

1 Introduction

The Moredun Group, are committed to comply with the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (DPA) in respect of personal data of the individuals whose information The Moredun Group collects and processes., including but not limited to staff, students, visitors, research participants, contractors and other third parties.

The responsibilities and accountability of The Moredun Group, including staff, students, visiting workers and/or other individuals working/undertaking a role on behalf of The Moredun group to comply fully with the UK GDPR and the DPA is set out within this policy.

This policy is applicable to all The Moredun Group's companies and departments who process personal data, including those performed on customers', clients', employees' and suppliers' and any other personal data the organisation processes from any source.

2 Definitions

The Moredun Group companies includes;

- **The Moredun Foundation**, registered in Scotland, No SC151865;
- **Moredun Research Institute**, registered in Scotland, No SC149440;
- **Moredun Scientific Limited**, registered in Scotland, No SC107439;
- **Pentlands Science Park Limited**, registered in Scotland, No SC148767;

The UK companies above have their registered office at Pentlands Science Park, Bush Loan, Penicuik, Midlothian, EH26 0PZ.

Wormvax Australia Pty Ltd, registered in Australia, ABN 59 162 279 987, registered office at Level 9, 575 Bourke Street, Melbourne, Vic 3000, Australia.

Two of the Moredun Group companies are also registered as charitable organisations: The Moredun Foundation, registered in Scotland, No: SC022515; Moredun Research Institute, registered in Scotland, No: SC022353.

Definitions used by the organisation (drawn from the GDPR)

Personal data – 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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – 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.

Data processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Officer – The Compliance Manager whose role is to; monitor the application of the GDPR, ensure compliance in all issues relating to the protection of personal data, advise and report to SMG any GDPR issues (including personal data breaches and subject access requests).

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – 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.

Personal data breach **–** 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.

Data subject consent **-** 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 them.

3 Purpose of Policy

This policy sets out the responsibilities, accountability and framework of The Moredun Group, including staff, students, visiting workers and/or other individuals working/undertaking a role on behalf of The Moredun group to follow to ensure compliance with the UK GDPR and the DPA.

This policy applies to all personal data we process regardless of format.

4 Responsibilities under the General Data Protection Regulation & the Data Protection Act

The Moredun Group is a data controller and/or data processor under the GDPR.

The Senior Management Group and all those in managerial or supervisory roles throughout The Moredun Group are responsible for developing and encouraging good information handling practices within there area of responsibility to ensure compliance with the UK GDPR, DPA and this policy.

Compliance with data protection legislation is the responsibility of all employees/ staff/ students and visiting workers of The Moredun Group who process personal data.

The Compliance Manager reports directly the Senior Management Group, who are accountable to Board of Directors of The Moredun Group for the management of personal data within The Moredun Group and for ensuring that compliance with data protection legislation and good practice can be demonstrated. The Compliance Manager has been designated responsible for managing compliance with this policy for the Moredun Group.

5 Questions to Ask Prior to Processing Personal Data

Prior to undertaking any processing of personal data whether this is a new programme, new software package, sharing data with a third party (e.g. cloud based hosting systems), research project or any other action that involves the use of personal data then the following questions should be asked:

- Do you really need to use the personal data?
- Can anonymised or pseudonymised data be used?
- Do you have a legal basis for processing the data? (See section 7)
- Has the privacy notice been provided to the data subject?
- How are you securing the personal data you are processing?
- Do you have the necessary safeguards in place if the personal data is being passed onto a third party or transferred outside the EEA?
- Have you completed a Data Protection Impact Assessment?

6 Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK GDPR. The Moredun Group's policies and procedures are designed to ensure compliance with the principles and all personal data shall be:

6.1 processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

6.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose (Purpose Limitation).

6.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).

6.4 accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay (Accuracy).

6.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the 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 individuals (Storage Limitation).

6.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Security, Integrity and Confidentiality).

6.7 responsible for and be able to demonstrate compliance with the principles above (6.1-6.6)

7 Lawful Basis for Processing

7.1 In order to process personal data you must have a valid lawful basis and this must be determined before you begin processing. At least one of the following must apply whenever personal data is processed:

- **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

  Note The UK GDPR sets a high standard for consent, which must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should

not generally be a precondition of signing up to a service. You must keep clear records to demonstrate consent. The UK GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw and offer them easy ways to withdraw consent at any time.

- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

- **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

- **Vital interests:** the processing is necessary to protect someone's life.

- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.) If this legal basis for processing is used, then a Legitimate Interest Assessment must be carried out. Contact the Compliance Manager for more information.

7.2 If you are processing special category data, you need to identify both a lawful basis for processing (6.1) and a special category condition for processing. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability. At least one of the following must apply whenever special category personal data is processed:

- **The data subject has given explicit consent to the processing** *(the requirements for explicit consent extend beyond that, which means that implied consent is not acceptable and the 'clear affirmative actions' that meet the requirements for ordinary consent are not sufficient. The key difference is that 'explicit' consent must be affirmed in a clear statement.*

- **The processing is necessary for employment law or social security law** purposes *(This legal basis is likely to be used in a HR context where an employee's sensitive personal data might be used to, for example, adapt a workstation.)*

- **The processing is necessary to protect vital interest** *(This replicates broadly the legal basis for processing ordinary personal data – if a person is incapable of giving consent due to, for example, being unconsciousness, medical data can be provided to the paramedics.)*

- **Processing by not-for-profit bodies or associations** *(it only applies to bodies or associations existing for political, philosophical, religious or trade union purposes.)*

- **Personal data manifestly made public** *(Sensitive personal data can, for example, be considered to have been made public by the data subject through a media interview published in a newspaper or broadcast on TV.)*

- **Establishment, exercise or defence of legal claims** (*This will cover most activities of lawyers acting on behalf of the Moredun and carrying out Moredun's instructions. Example -HR processes a perspective employee's nationality information with a view to seeking legal advice on a visa application.*

- **Substantial public interest** *(Additional legislation has been created to make the processing of special categories of personal data legal for the purposes of providing counselling services and to detect and investigate malpractice.)*

- **Medical purposes and the provision of health or social care** *(This legal basis will be used in situations where the processing is necessary for the purposes of occupational medicine and social care as well as preventative medicine and diagnosis, the provision of health care and treatment and also the management of health or social care systems and services.)*

- **Public health** *(This legal basis permits the processing sensitive personal data in cases of threats to health from infectious diseases. Moredun will have the legal duty to notify the government to prevent the spread of the disease.)*

- **Archive, statistical and research purposes** *(If at all possible, all personal data – both special categories and ordinary personal data – should be anonymised for archiving, research and statistics. If that is not possible, then data protection legislation allows the activities to be carried out under suitable safeguards*

8 Data Security

All Employees/Staff are responsible for ensuring that any personal data that The Moredun Group holds and for which they are responsible, is kept securely and is not under any condition disclosed to any unauthorised third party.

All staff must read and acknowledge The Moredun group Code of Practice Covering use of Computer Facilities and Communications Systems.

The Moredun Group Head of ICT Services is responsible for managing information security including emerging threats and security awareness training. Developing and maintaining a high level of resilience over the Group's information systems including backup and recovery.

9 Privacy Notice

The Moredun Group is committed to protecting and respecting your privacy and complies with its obligations under the General Data Protection Regulations by keeping personal data up to date. When The Moredun Group collects personal data we must provide data subjects with a "privacy notice" this provides clear and transparent information to individuals about how their personal data are collected, used or otherwise processed, and to what extent personal data are, or will be, processed. Any data processing must be consistent with the purpose and detailed in the privacy notice.

A staff fair processing notice is in place for The Moredun Group Staff detailing how their information is processed and for what purpose.

10 Data Retention

The Moredun Group shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected. This is applicable to all personal data regardless of where it is stored e.g. core systems, laptops, desk top PCs, mobile devices, paper records.

Data retention periods are based on both business and legal requirements and are documented within the privacy notice and staff fair processing notice. If more information is required then contact the Compliance Manager.

The Moredun Group may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

When the data is no longer required then it must be deleted, destroyed or fully anonymised at the end of the retention period or archived as detailed above.

11 Data Protection by Design and Default

The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. In essence, this means you have to integrate data protection into your processing activities and business practices, from the design stage right through the lifecycle. Data protection by design is about considering data protection and privacy issues upfront in everything you do.

12 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows The Moredun Group to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks. As the use of technology and the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases.

A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also if there is a change to the risk of processing for an existing project a review should be carried out. In the context of this guidance a project could include the development or enhancement of any activity, function or processing such as a system, database, programme, application, service or scheme. The time and effort put into carrying out the DPIA should be proportionate to the risks. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Your DPIA must:
- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

13 Anonymisation and Pseudonymisation

13.1 Anonymisation

Anonymisation is the process of removing personal identifiers permanently, both direct and indirect, that may lead to an individual being identified. Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR since it is no longer personal data..

13.2 Pseudonymisation

Pseudonymisation is the processing of personal information 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 information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an individual being identified.

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.

14 Handling Research Data

Prior to commencing any research project think about the data you will be processing and whether this is information that **relates** to a living person and which **identifies** that person, either **directly or indirectly** (e.g. farm postcode, animal tag number). If the data can directly

or indirectly identify a person, then this is personal data and a Data Protection Impact Assessment should be carried out before the project starts.

Where the research project legal basis for processing Person data is consent then consent must be sought this can be done by utilising the on-line Jisc survey platform to gain and manage consent. Alternative methods may also be employed, such as signing of a privacy statement.

All data subjects must be provided with a privacy notice and a participant information sheet.

15 Data Subject Rights

The UK GDPR and DPA provides data subjects with more control over their data as well as a better understanding of what their data is being used for. As a result data subjects have certain data protection rights under the UK GDPR and DPA that if infringed allow the data subject to take legal action against data controllers and data processors and seek compensation for damages.

There are eight (8) rights that belong to data subjects, namely:

- **to be informed** - organisations need to tell individuals what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language

- **to access** - individuals can submit subject access requests, which oblige organisations to provide a copy of any personal data they hold concerning the individual. Organisations have one month to produce this information, although there are exceptions for requests that are manifestly unfounded, repetitive or excessive.

- **to rectification** - if an individual discovers that the information an organisation holds on them is inaccurate or incomplete, they can request that it be updated. As with the right of access, organisations have one month to do this, and the same exceptions apply.

- **to erasure** - individuals can request that organisations erase their data in certain circumstances – for example, when the data is no longer necessary, the data was unlawfully processed, or it no longer meets the lawful ground for which it was collected. This includes instances where the individual withdraws consent. The right to erasure is also known as 'the right to be forgotten'

- **to restrict processing** - individuals can request that an organisation limits the way it uses personal data. It's an alternative to requesting the erasure of data and might be used when an individual contests the accuracy of their personal data. An individual can also exercise this right when they no longer use the product or service for which it was originally collected, but the organisation needs it to establish, exercise or defend a legal claim.

- **to data portability** - individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent.

- **to object** - individuals can object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority. Organisations must stop processing information unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual. They can also refuse this right if the processing is for the establishment or exercise of defence of legal claims.

- **related to automated decision making including profiling** - the GDPR includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about individuals. There are strict

rules about this kind of processing, and individuals are permitted to challenge and request a review of the processing if they believe the rules aren't being followed.

If you receive a subject access request, or other data subject right then these should be forwarded to the Compliance Manager or emailed to info@moredun.ork.uk

16 Data Sharing

16.1 Internal

When personal data is transferred internally the recipient must only process the data in the same manner as the original purpose for which the data was collected. If this is not the case then a new privacy notice will need to be provided to the data subject and a data processing impact assessment carried out.

16.2 External

When personal data is transferred externally a data sharing agreement is required between The Moredun Group Company and the third party, this must detail the legal basis for processing and signed by the two parties. There are legal exceptions to this e.g. Inland revenue, Department of Work & Pensions

17 Transfers of Personal Data Outside the EEA

17.1 Restricted Transfer covered by Adequacy Regulation

The UK GDPR contains rules on the transfer of personal data to receivers located outside the UK, which are separate controllers or processors and legally distinct from you. These rules apply to all transfers, no matter the size of transfer or how often you carry them out. The transfer of personal data to these receivers located outside the UK are referred to as a 'restricted transfer'.

- On that basis, the UK GDPR contains rules about transfers of personal data to receivers located outside the UK. People's rights about their personal data must be protected or one of a limited number of exceptions must apply.
- The transfer rules apply where the receiver is a separate controller or processor and legally distinct from the sender. The receiver can be a separate sole trader, partnership, company, public authority or other organisation, and includes separate companies in the same group.
- The transfer rules do not apply where the receiver is an employee of the sender, or the sender and receiver are part of the same legal entity, such as a company.
- We refer to a transfer of personal data to these receivers located outside the UK as a 'restricted transfer'.
- Before making a restricted transfer you should consider whether you can achieve your aims without actually sending personal data.
- If you make the data anonymous so that it is never possible to identify individuals, it is not personal data. If this is the case, then the restrictions do not apply and you are free to transfer the anonymised data outside the UK.

You may make a restricted transfer if the receiver is located in a third country or territory, or is an international organisation, or in a particular sector in a country or territory, covered by UK 'adequacy regulations'.

The UK has adequacy regulations about the following countries and territories:

Countries covered by adequacy regulations

17.2 Restricted Transfer covered by Appropriate Safeguards (Transfer Mechanisms)

If there are no UK adequacy regulations about the country, territory, international organisation, or particular sector in a country or territory for your restricted transfer, you should then find out whether you can make the transfer subject to 'appropriate safeguards' (transfer mechanisms). The list of appropriate UK GDPR safeguards (transfer mechanisms) are detailed below. Each

safeguard (transfer mechanism) ensures that both you and the receiver of the restricted transfer are legally required to protect people's rights and freedoms about their personal data.

Before relying on one of the transfer mechanisms to make a restricted transfer, you must be satisfied that the relevant protections in the UK GDPR are not undermined for people whose data is transferred. You should do this by undertaking a risk assessment and if your assessment is that the transfer mechanism does not provide the required level of protection, before making the transfer you must take extra steps and protections so that it does provide the right level of protection.

Transfer Mechanisms

- A legally binding and enforceable instrument between public authorities or bodies
- UK Binding corporate rules (UK BCRs)
- Standard data protection clauses
- An approved code of conduct
- Certification under an approved certification scheme
- Contractual clauses authorised by the ICO
- Administrative arrangements between public authorities or bodies

18 Direct Marketing

Direct marketing covers the promotion of aims and ideals as well as the sale of products and services. This means that the rules will cover not only commercial organisations but also not-for-profit organisations (eg charities).

The Privacy and Electronic Communications Regulations (PECR) sit alongside the UK GDPR and the Data Protection Act and cover several areas including marketing by electronic means, (marketing calls, texts, emails and faxes) and the use of cookies or similar technologies that track information about people accessing a website or other electronic service.
Since The Moredun Foundation and The Moredun Foundation Equine Grass Sickness Fund are registered charities relying on donations and support from others in order to achieve our mission we may contact members and supporters with communications and fundraising material.

We want our supporters to be the first to know about the latest research and innovations from The Moredun Group. Therefore we may contact them through post, email and digital platforms however we may also contact them via telephone calls. We will only send them email communications with your explicit consent and their will have the option to opt out of any of our marketing communications at any time.

Every time The Moredun Group undertakes direct marketing we will ensure that we comply with the legislations and if an individual requests to opt-out then we will cease all direct marketing activities.

19 Data Protection Training

All Moredun Group staff receive GDPR training and refresher training as all staff are responsible managing the personal information, they use in line with Moredun's policies and complying with the UK GDPR, the DPA and any other applicable legislation.

20 Data Protection Breaches

A 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;

- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Whilst The Moredun Group makes every effort to avoid data protection breaches it is realised that accidental breaches may occur. If a breach occurs then this should be reported immediately to the Compliance Manager who will raise the data breach in Q-Pulse using the Data Protection Breach template and investigate.

If this is a notifiable data protection breach then The Moredun Group are required to notify the Information Commissioners Office as soon as possible but not later than 72 hours after becoming aware of the breach.

The Compliance Manager keeps a register of all data protection incidents and breaches.

21 The Data Protection Officer

Moredun do not have the specified number of employees and is not a public body, therefore designation of a data protection officer is not required. However, he Moredun Group has designated a Compliance Manager to manage the compliance with the UK General Data Protection Regulation and the Data Protection Act throughout the Moredun Group.

The Compliance Manager can be contacted directly or via the info@moredun.org.uk email address.