# Data Protection Policy

## 1. GENERAL STATEMENT

1.1 This policy applies to the Serocor Group of companies. You are a Client or customer of, an employee or contractor of, or a Supply Chain Partner to, at least one Serocor Group company. Any reference to "Serocor" or "the Serocor Group" or "we" or "us" or "our" refers to that Serocor Group company and, where relevant, the other companies within the Serocor Group.

## 2. CONTENTS

2.1 This policy has been layered into different sections so it can be easily understood. Please use the below section headings to help guide you:



## 3. DEFINITIONS

3.1 In this policy, the following definitions apply:

- "**Automated Decision-Making**" means a decision made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual;
- "**Automated Processing**" means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing;
- "**Client**" means any organisation in which we provide our services to;
- "**Consent**" means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to him or her;

- "**Criminal Conviction Data**" means Personal Data consisting of information as to the commission or alleged commission by him of any offence; any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;
- "**Data Controller**" means the organisation that determines the purposes for which, and the manner in which, any Personal Data is Processed;
- "**Data Privacy Impact Assessment**" (**DPIA**) means the tools and assessments used to identify and reduce risks of a data processing activity. DPIAs should be conducted for all major system or business change programs that involve the Processing of Personal Data;
- "**Data Processor**" means the organisations that carries out the instructions of the Data Controller;
- "**Data Protection Legislation**" means the Data Protection Act 1998, and amendment or re-enactment thereof, as well the General Data Protection Regulation (GDPR) and any other applicable legislation in relation to the protection of Personal Data;
- "**Data Protection Officer**" or "**DPO**" means the person or team designated or appointed with responsibility for data protection compliance;
- "**Data Subject**" means a living individual who is the subject of Personal Data;
- "**Explicit Consent**" means any Consent required and/or obtained in relation to the use of:
    - Special Categories of Personal Data;
    - Automated Decision-Making;
    - Overseas transfers in the absence of adequate safeguards;
- "**Personal Data**" means data - stored electronically, on a computer, or in paper-based filing systems - which relates to a living individual who can be identified from that data or from that data and other data in the Data Controller's possession;
- "**Personal Data Breach**" means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect Personal Data. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach;
- "**Privacy by Design**" means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;
- "**Processing**" or "**Process**" refers to any action or activity involving Personal Data, including obtaining, handling, recording, viewing, copying, amending, storing, disclosing, transporting, deleting or destroying Personal Data;
- "**Related Policies**" means Serocor's policies, operating procedures or processes relating to this Data Protection Policy which are designed to protect Personal Data.
- "**Special Categories of Personal Data**" means Personal Data consisting of information as to the Data Subject's racial or ethnic origin; political opinions; religious beliefs or

other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life;

- "**Staff**" means all employees, executive and non-executive directors, internal contractors and temporary staff of Serocor;
- "**Supervisory Authority**" means a supervisory authority or regulator which is concerned by the processing by the processing of personal data because:
  - The Data Controller or Data Processor is established on the territory of the Member State of that supervisory authority;
  - Data Subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
  - A complaint has been lodged with that supervisory authority;
- "**Supply Chain Partners**" means any:
  - Suppliers and business partners who provide support services;
  - Professional advisors including lawyers, bankers, auditors and insurers who provide legal, banking, accounting and insurance services;
  - HM Revenue & Customs, regulators and authorities who require reporting of processing activities in certain circumstances;
  - Other law enforcement agencies in connection with any investigation to help prevent unlawful activity or as otherwise required by applicable law;
  - Any other third parties or supply chain partners we may require access to and/or process personal data;
- "**Transparency Notices**" means separate notices setting out information that may be provided to Data Subjects when we collect and use information about them. These notices may take the form of general privacy statements (for example, the Serocor's Group Transparency Notice available on our Group Privacy Centre – http://www.serocor.com/PrivacyCentre.aspx) or they may stand-alone, one time privacy statements covering Processing related to a specific purpose (for example, prospective employees).

## 4. POLICY STATEMENT

4.1 We hold and Process Personal Data about current, past and prospective staff, candidates, contractors, clients, supply chain partners and other Data Subjects for recruitment, administrative and commercial purposes. The information, which is held in paper format or electronically on computers or other media and devices, is subject to certain legal safeguards as outlined in the Data Protection Legislation. The Data Protection Legislation sets out and imposes strict obligations on how Personal Data can be used.

4.2 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in us and our supply chain which will provide for successful business operations.

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

4.3 This policy sets out Serocor's rules on data protection and the legal conditions that must be satisfied in relation to the Processing of Personal Data.

4.4 This policy applies to all Staff and, where applicable, to all Clients and Supply Chain Partners ("you" or "your"). You must fully comply with this policy. You must read, understand and comply with this policy when Processing Personal Data on our behalf and attend training on its requirements, where applicable. This policy sets out what we expect from you in order for Serocor to comply with applicable law.

4.5 If you are a Client or a Supply Chain Partner, please refer to the "Client and Supply Chain Partners" section for more information.

4.6 This policy should be read in conjunction with the other Related Policies, which are available on the Serocor intranet or as otherwise made available to you, to help you interpret and act in accordance with this policy.

4.7 This policy (together with any Related Policies) cannot be shared with any unauthorised third party without prior written authorisation from Serocor.

4.8 The Personal Data held by Serocor is processed under Serocor's registration with the Information Commissioner's Office (ICO), the UK's Supervisory Authority for data protection regulation. If you use Serocor's Personal Data for any unauthorised purposes or if you use Serocor's Personal Data after you leave Serocor, you will be acting outside of Serocor's ICO registration which may mean you are committing a criminal offence.

4.9 Each legal entity in the Serocor Group is registered as a separate data controller with the ICO:

- Advanced Resource Managers Limited (ICO Registration Number: Z9352884)
- Advanced Resource Managers IT Limited (ICO Registration Number: Z6525711)
- Advanced Resource Managers Engineering Limited (ICO Registration Number: Z8922161)
- Optamor Limited (ICO Registration Number: ZA005342)
- Serocor Projects Limited (ICO Registration Number: ZA005344)

## 5. CLIENTS AND SUPPLY CHAIN PARTNERS

### 5.1 Clients

- If you are a Client, it is your responsibility to ensure that you are compliant with the Data Protection Legislation.
- We expect you to adhere to and comply with your obligations under the Data Protection Legislation and have in place a data protection policy which sets out how you

handle Personal Data of your customers, employees, workers, suppliers and other third parties.

- Please read this policy for further information about how we handle Personal Data.

5.2 **Supply Chain Partners**

- If you are part of our supply chain, it is your responsibility to ensure that you are compliant with the Data Protection Legislation.
- We expect you to adhere to and comply with your obligations under the Data Protection Legislation and have in place a data protection policy which sets out how you handle Personal Data of your customers, employees, workers, suppliers and other third parties.
- If you are a Data Processor on behalf of the Serocor Group, we expect you to adhere to and comply with the provisions set out this policy, which forms part of your working relationship with us, in conjunction with your obligations under the Data Protection Legislation.

## 6. THE DATA PROTECTION PRINCIPLES

6.1 We adhere to the principles relating to Processing of Personal Data set out in the Data Protection Legislation which requires Personal Data to be:

- Processed lawfully, fairly and in a transparent manner in relation to a Data Subject (Lawfulness, Fairness, Transparency);
- Collected for specified, explicit and legitimate purposes (Purpose Limitation);
- Adequate, relevant and limited to what is necessary for the purpose of the Processing (Data Minimisation);
- Accurate and, where necessary, kept up to date (Accuracy);
- Retained for no longer than is necessary for the purpose of the Processing (Storage Limitation);
- Processed using appropriate technical or organisational measures to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing (Security, Integrity and Confidentiality);
- Not transferred to another country or territory without appropriate safeguards being in place (Transfer Limitation); and
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights).

6.2 We are responsible for and must be able to demonstrate compliance with the data protection principles above (Accountability).

## 7. LAWFULNESS, FAIRNESS, TRANSPARENCY

7.1 The Data Protection Legislation does not prevent the Processing of Personal Data, but ensures that it is done fairly and lawfully, for a specified purpose and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is, the purpose for which the Personal Data is to be processed and the identities of anyone to whom the Personal Data may be disclosed or transferred.

7.2 The Data Protection Legislation allows Processing for specific purposes and the lawful basis being relied upon for each Processing activity must be clearly identified, documented and easily accessible.

## 8. PURPOSE LIMITATION

8.1 Personal Data must only be collected and Processed for the specified, explicit and legitimate purposes which have been notified to the Data Subject. It must not be further Processed in any manner which is incompatible with those purposes. Personal Data must not be collected for one purpose and then used for another.

8.2 You must not Process Personal Data for any purpose other than what is required as part of your obligations.

8.3 If it becomes necessary to change the purpose for which the Personal Data is Processed, the Data Subject must be informed of the new purpose before any Processing occurs. The Data Subject has the right to object to the new purpose.

## 9. DATA MINIMISATION

9.1 Personal Data must only be collected to the extent that it is required for the specific purpose notified to the Data Subject. Personal Data must be adequate, relevant and limited.

9.2 You may only Process Personal Data when required to do so as part of your obligations. You cannot Process Personal Data for any reason unrelated to your obligations and you must ensure that any Personal Data collected is adequate and relevant for the intended purposes. It must not be excessive.

9.3 When Personal Data is no longer needed for a specified purpose(s) and there is no other lawful basis or requirement to hold the Personal Data, it must be deleted or anonymised. Please refer to the Storage Limitation section of this policy for further information.

## 10. ACCURACY

10.1 Personal Data must be accurate and kept up-to-date. Personal Data which is incorrect or misleading is not accurate and steps must therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

10.2 Where necessary, Personal Data must be corrected or deleted without any undue delay when inaccurate.

10.3 You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

## 11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which it was collected.

11.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the lawful basis for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

11.3 We will maintain specified retention periods to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such Personal Data to be kept for a minimum time. You must comply with our instructions or as otherwise required under any relevant legislation.

11.4 You will take all reasonable steps to destroy or erase all Personal Data that is no longer required in accordance with all of our instructions or as otherwise required under any relevant legislation. This includes requiring third parties to delete such data, where applicable.

11.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined.

## 12. SECURITY, INTEGRITY, CONFIDENTIALITY

PROTECTING PERSONAL DATA

12.1 There must be appropriate technical and organisational security measures in place to prevent the unlawful or unauthorised Processing of Personal Data, and to prevent the accidental loss of, damage to or destruction of, Personal Data.

12.2 We have implemented and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we hold or maintain on behalf of others and identified the relevant risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

12.3 You are responsible for protecting the Personal Data that you hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, damage to or destruction of, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Conviction Data from loss and unauthorised access, use or disclosure.

12.4 You must follow all procedures put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

12.5 You must maintain data security by protecting the Confidentiality, Integrity and Availability of the Personal Data, defined as follows:

- "Confidentiality" means that only people who have a need to know and are authorised to use the Personal Data can access it.
- "Integrity" means that Personal Data is accurate and suitable for the purpose for which it is Processed.
- "Availability" means that authorised users are able to access the Personal Data when they need it for authorised purposes.

12.6 You must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards implemented and maintained in accordance with the Data Protection Legislation and relevant standards to protect Personal Data.

REPORTING A PERSONAL DATA BREACH

12.7 The Data Protection Legislation requires any Personal Data Breach to be notified to the applicable Supervisory Authority and, in certain instances, the Data Subject.

12.8 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable Supervisory Authority where we are legally required to do so.

12.9 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You must ensure that you preserve all evidence relating to the potential Personal Data Breach and immediately email: DPO@serocor.com.

## 13. TRANSFER LIMITATION

13.1 Data Protection Legislation restricts data transfers to countries outside the European Economic Area ("EEA") in order to ensure that the level of data protection afforded to individuals by the Data Protection Legislation is not undermined. Personal Data originating in one country is transferred across borders when it is transmitted, sent, viewed or accessed in or to a different country.

13.2 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

- Appropriate safeguards are in place such as the standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained by emailing DPO@serocor.com;
- The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the Data Protection Legislation, including: the performance of a contract between us and the Data Subject; reasons of public interest; to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and, in some limited cases, for our legitimate interests.

13.3 You must comply with our guidelines on transferring Personal Data to countries outside the EEA.

13.4 Any queries or issues relating to the transfer of Personal Data to countries outside the EEA should be referred to DPO@serocor.com.

## 14. DATA SUBJECTS' RIGHTS

14.1 Personal Data must be processed in line with Data Subjects' Rights. Data Subjects have the following rights with respect to Personal Data:

- **Right to be informed**: the right to be made aware of how Personal Data is used.
- **Right to withdraw your Consent**: the right to withdraw any Consent to the Processing at any time.
- **Right of access**: the right to access the Personal Data held on the Data Subject including any supplementary information.
- **Right to rectification**: the right to have any Personal Data rectified if it is inaccurate or incomplete.
- **Right to erasure**: the right 'to be forgotten' and to request the deletion or removal of Personal Data held on the Data Subject where it is no longer necessary to continue Processing it.
- **Right to restrict processing**: the right to block any Processing of Personal Data where there is a dispute in relation to the accuracy or Processing of the Personal Data.
- **Right to data portability**: the right to obtain, re-use and transfer the Personal Data held on the Data Subject for the Data Subject's own purposes.
- **Right to object**: the right to object to how the Personal Data is Processed, where applicable.
- **Rights related to Automated Decision-Making**: the right not to be subject to a decision based solely on Automated Decision-Making.

14.2 You must verify the identity of an individual requesting Personal Data under any of the rights listed above.

14.3 You must immediately forward any Data Subject request you receive to DPO@serocor.com.

## 15. ACCOUNTABILITY

15.1 We are all responsible for, and must be able to demonstrate, compliance with the data protection principles. As part of the Accountability principle, we have, and you must have, adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including:

- Appointing a suitably qualified Data Protection Officer (if applicable) for data protection matters;
- Implementing appropriate technical and organisational measures in an effective manner when Processing Personal Data and completing DPIAs where Processing presents a high risk to the rights and freedoms of Data Subjects;
- Integrating data protection into internal documents including this policy, Related Policies, and any Transparency Notices;
- Regularly training staff on Data Protection Legislation, this policy, Related Policies and data protection matters including, for example, Data Subject's rights, the lawful bases for Processing Personal Data, DPIA and Personal Data Breaches. We will, and you must, maintain a record of training undertaken by Staff; and
- Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

## 16. RECORD KEEPING

16.1 Data Protection Legislation requires us to keep full and accurate records of all our Processing activities.

16.2 We will, and you must, keep and maintain accurate records reflecting any Processing, including records of Data Subjects' Consents and our procedures for obtaining Consents.

16.3 These records should include, at a minimum, the name and contact details of the Data Controller and the Data Protection Officer (if applicable), clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

## 17. TRAINING AND AUDIT

17.1 We are required to ensure that all Staff and, where relevant, Supply Chain Partners have undergone adequate training to enable them to comply with the Data Protection Legislation and our internal processes and procedures. We will regularly test our systems and processes to assess compliance.

17.2 We will, and you must, regularly review all the systems and processes under our control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

## 18. DATA PROTECTION IMPACT ASSESSMENT

18.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

18.2 Where applicable, a DPIA will be conducted by the Legal Team to assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- The nature, scope, context and purposes of Processing;
- The risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing; and
- The cost of implementation.

18.3 We will conduct DPIAs in respect to high risk Processing and/or when implementing major system or business change programs involving the Processing of Personal Data including:

- The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and Automated Decision Making;
- Large scale Processing of Special Categories of Personal Data; and
- Large scale, systematic monitoring of a publicly accessible area.

18.4 A DPIA must include:

- A description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- An assessment of the necessity and proportionality of the Processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

18.5 You will ensure that you make yourself available to assist the Legal Team with any DPIA, where required.

18.6 You must comply with our guidelines on DPIA and Privacy by Design.

## 19. AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING

19.1 Automated Decision-Making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- A Data Subject has Explicitly Consented;
- The Processing is authorised by law; or
- The Processing is necessary for the performance of or entering into a contract.

19.2 If certain types of Special Categories of Personal Data is being processed, then grounds (b) or (c) will not be allowed but such Special Categories of Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

19.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

19.5 A DPIA must be carried out before any Automated Processing or Automated Decision-Making activities are undertaken.

19.6 We do not conduct any Automated Decision-Making; however we do carry out profiling in order to provide our services to our candidates, contractors and Clients.

## 20. DIRECT MARKETING

20.1 We are subject to certain rules and data protection laws when marketing to our customers, including candidates, Clients and our Supply Chain Partners.

20.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing business customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

20.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

20.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

20.5 You must comply with our guidelines on direct marketing to candidates, Clients and our Supply Chain Partners.

## 21. SHARING PERSONAL DATA

21.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

21.2 You may only share the Personal Data we hold with another employee, agent or representative of the Serocor Group if the recipient has a job-related "need to know" and the transfer complies with any applicable cross-border transfer restrictions.

21.3 You may only share the Personal Data we hold with third parties, such as our Supply Chain Partners if:

- They have a "need to know" the information for the purposes of providing the contracted services;
- Sharing the Personal Data complies with the Transparency Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains approved third party clauses has been obtained.

21.4 If you want to share personal data with a third party for any reason, or if a third party asks you to disclose Personal Data to them, you must email DPO@serocor.com for further advice.

21.5 You must comply with our guidelines on sharing data with third parties.

## 22. DATA PROTECTION DO'S AND DON'TS

22.1 To ensure we comply with our obligations under Data Protection Legislation, we have set out some clear guidelines below. This is primarily aimed at Staff, but our Supply Chain Partners are also included where appropriate. Please read the following very carefully:

- You must only Process Personal Data if you have a lawful basis to do so;You must only Process Personal Data in a way that falls within the Data Subject's reasonable expectations, and which is compatible with the original purpose(s) for which the Personal Data was collected;

- You must only collect Personal Data that is necessary for the particular purpose. You must not collect excessive or irrelevant Personal Data;
- You must help to make sure the Personal Data we hold is up-to-date. For example, you should check with candidates, contractors, Clients and Supply Chain Partners that the information we hold on them is up-to-date. You should update it on our systems as appropriate;
- Do not delete or destroy any Personal Data. The deletion or destruction of Personal Data will be carried out in line with our data retention policies and by IT Helpdesk;
- You must make sure Personal Data is kept secure. If any Personal Data is lost or stolen, or if any device holding Personal Data is lost or stolen, you must notify your Line Manager, the IT Helpdesk and immediately email: DPO@serocor.com;
- If any Personal Data is disclosed to a third party in breach, or potential breach, of the Data Protection Legislation, you must notify your Line Manager, the IT Helpdesk and immediately email: DPO@serocor.com;
- If you are asked to provide Personal Data over the telephone, you must take steps to verify the identity of the caller. If you have any doubt over the caller's identity, you must not disclose any Personal Data;
- Do not download any Personal Data onto a laptop or portable electronic device unless you have permission from your Line Manager and IT Helpdesk to do so. You must sign and comply with the relevant Related Policies to enable you to download any Personal Data, for example the BYOD Policy and the Remote Access Policy;
- If any person indicates that they do not want to be contacted by us, you must email: unsubscribe@serocor.com immediately so that appropriate filters can be put in place.

22.2 The above list is not intended to be exhaustive. It is up to you to make sure you comply with the Data Protection Legislation in line with our policies and the training given to you.

## 23. RESPONSIBILITY FOR THE POLICY

23.1 The Serocor board of directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

23.2 The Legal Team has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures.

23.3 Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it and the issue of data protection.

23.4 It is the responsibility of all Staff who have access to Personal Data to ensure that they comply with this policy and any other Related Policies.

## 24. COMPLIANCE WITH THE POLICY

24.1 Your awareness in matters relating to data protection is a critical element of this policy. New members of Staff will be given an explanation of the individual responsibilities for data protection as part of the induction process. All other external third parties subject to this policy are required to take the necessary steps to ensure that they understand its obligations under Data Protection Legislation and this policy.

24.2 You are responsible for and must comply with the security arrangements for the system(s) you use. You must read, understand and follow the guidelines set out in this policy as updated from time to time by email, intranet or other notice.

24.3 If you have any questions or concerns about this policy, please refer all queries to DPO@serocor.com.

24.4 If you believe that this policy has not been followed by any person, you must raise your concerns with your Line Manager and email DPO@serocor.com.

24.5 If you believe there has been a Personal Data Breach, you must email DPO@serocor.com immediately. You must not take any further action without the Legal Team's approval.

## 25. BREACHES OF THE POLICY

25.1 For Staff: It is your responsibility to ensure that you are familiar with and abide by the terms of this policy. If you misuse or breach this policy, or otherwise breach the Data Protection Legislation, you will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

25.2 For Staff: A breach of this policy may also result in legal claims against you and/or Serocor, and will be regarded as a disciplinary matter and dealt with in line with our disciplinary policy and procedure. Any Staff whose conduct breaches this policy in any way will be subject to disciplinary action in accordance with Serocor's disciplinary procedure up to, and including, summary dismissal. Any damage caused to Serocor and/or its reputation or which could or be likely to cause any damage shall be considered gross misconduct.

25.3 For Staff, Clients and Supply Chain Partners: If you knowingly or recklessly breach this policy or the Data Protection Legislation, you may be held criminally liable. Where appropriate, we will assist the relevant authorities with any investigation and/or prosecution to ensure that the appropriate penalty is charged against you.

25.4 If you are a Client or a Supply Chain Partner, we may terminate our relationship with you and report your activities to the relevant authority if you breach this policy or otherwise breach the Data Protection Legislation.

## 26. STATUS OF THIS POLICY AND REVIEWS

26.1 This policy will be reviewed by the Legal Team on a regular basis (at least annually) to take account of changes in the law and guidance issued by the ICO and therefore may be amended from time to time.