DATA PROTECTION AND SECURITY POLICY

CONTENTS

1. About this Policy

1.1 The types of Personal Data that Medecon Healthcare Ltd., Reg. No: 06584490**,**Regd Office: 15 Shrubbery Road, High Wycombe, Buckinghamshire, England, HP13 6PW may be required to handle include information about current, past and prospective suppliers, customers, contractors, and any other users of any of our services and others that we communicate with for the purposes of carrying out our business and services. The Personal Data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards including those specified in the General Data Protection Regulation, Regulation (EU) 2016/679 (the **GDPR**) and other regulations.

1.2 This policy and any other documents referred to in it sets out the basis on which we will process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or other sources. Data Users are obliged to comply with this policy when Processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action. This policy focuses on our obligations as a Data Controller and we may be under different or additional obligations in respect of any Processing which we carry out as a Data Processor.

1.3 This Policy will be reviewed at least once a year and periodically updated by the Data Protection Officer to reflect any changes in legislation or in our methods or practices. The current issue of the Policy will be available from our website at Medecon Healthcare.com or from our Data Protection Officer.

2. Definitions

2.1 **Data Subjects** means all living identifiable individuals about whom we hold Personal Data. A Data Subject need not be an EU national or resident. All Data Subjects have legal rights in relation to their personal information.

2.2 **Personal Data** means data relating to a living individual who can be identified, directly or indirectly, from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behavior.

2.3 **Data Controllers** are the people who, or organizations which, determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the GDPR. **Data Users** are those of our employees, agents and contractors whose work involves Processing Personal Data. Data Users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.4 **Data Processors** include any person or organization that processes Personal Data on our behalf and on our instructions. Employees of Data Controllers are excluded

from this definition but it could include suppliers that handle Personal Data on our behalf.

2.5 **Website** means our website at https://www.medecon.co.uk

2.6 **Processing** is any activity or set of activities which is performed on Personal Data or sets of Personal Data, whether or not by automated means. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

2.7 **Profiling** means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, locations or movements.

2.8 **Privacy Policy** the most recent version of our policy, available via the Website, relating to the collection, storage and use of Personal Data (as amended from time-to- time).

2.9 **Pseudonymization** means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. Note, pseudonymized data is still Personal Data.

2.10 **Sensitive Personal Data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. The GDPR includes biometric data and genetic data as Sensitive Personal Data. Sensitive Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

2.11 **Services** means: (i) access to the relevant services provided by medecon Healthcare (ii) Products and services provided to Customer by Medecon Healthcare.

3. Accountability

3.1 The GDPR accountability principle requires organizations to be able to demonstrate compliance with data protection requirements. We need to ensure data protection compliance is integrated into any new technology planning or new Processing activities.

3.2 The Data Protection Officer is responsible for ensuring compliance with the GDPR and with this policy. That post is held by Mr. David Jones, Compliance Manager, contact email address is:service@medecon.co.uk . Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

3.3 The Data Protection Officer will be an independent officer, appointed to carry out the following tasks on behalf of Medecon Healthcare:

(a) Inform and advise us or our Data Processors who carry out Processing activities of their obligations under the GDPR or particular jurisdiction data protection provisions.

(b) Monitor our compliance with the GDPR, or relevant data protection legislation which may apply to us and monitor our compliance with our policies or the policies of the Data Processor's.

(c) Provide advice where requested with regards to the data protection impact assessment and monitor its performance.

(d) To cooperate with the supervisory authority and act as a contact point for the supervisory authority on issues relating to Processing.

3.4 Data Subjects may contact the Data Protection Officer with regards to all issues related to Processing of their Personal Data and in respect of their rights under the GDPR.

3.5 All Medecon Healthcare employees have a responsibility to comply with the GDPR and are required to complete appropriate training to ensure compliance with this policy. To ensure the Data Protection Officer has the necessary support in carrying out their obligations, this position reports to Medecon Healthcare's Management team.

4. Data Protection Principles

Anyone Processing Personal Data must comply with principles of good practice.
These provide that Personal Data must be:

(a) Processed fairly, lawfully and in a transparent manner in relation to individuals.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

(d) Accurate and where necessary, kept up to date. Where Personal Data is inaccurate with regards to the purpose for which it is processed, every reasonable step must be taken to either erase or rectified it without delay.

(e) Not kept longer than necessary for the purpose for which the Personal Data is processed.

(f) Processed in line with Data Subjects' rights.

(g) Processed in a manner that ensures appropriate security of the Data Subject, including protection against unauthorized Processing and accidental loss, destruction or damage.

(h) Not transferred to people or organizations situated in countries without adequate protection without putting in place appropriate safeguards.

5. Fair and Lawful Processing

5.1 The GDPR is not intended to prevent the Processing of Personal Data, but to ensure that it is done fairly, transparently and without adversely affecting the rights of the Data Subject. The specific purposes for which Personal Data is being processed should be explicitly and legitimately communicated to the Data Subject's and should be determined at the time of the collection of the Personal Data.

5.2 For Personal Data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the Data Subject's consent to the Processing, or that the Processing is necessary for the performance of a contract with the Data Subject, for the compliance with a legal obligation to which the Data Controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When Sensitive Personal Data is being processed, additional conditions must be met. When Processing Personal Data as Data Controllers in the course of our business, we will ensure that those requirements are met.

6. Processing for Limited Purposes

6.1 In the course of our business, we may collect and Process Personal Data. This may include data we receive directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub- contractors in technical, payment and delivery services, credit reference agencies and others).

We will only Process Personal Data for the specific purposes set out in our Privacy Policy or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the Data Subject when we first collect the data. We will continually review our notices to ensure that they accurately reflect our Processing activities and where we Process the data for a new purpose which was not indicated in the initial notification, then we will provide a new notice to cover this.

7. Categories of Data Subjects

7.1 Medecon Healthcare collects and processes a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number, date of birth and gender;
- The terms and conditions of your employment;
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with Medecon Healthcare;
- Information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- Details of your bank account and national insurance number;
- Information about your marital status, next of kin, dependents and emergency contacts;
- Information about your nationality and entitlement to work in the UK;
- Information about your criminal record;
- Details of your schedule (days of work and working hours) and attendance at work;
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- Assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- Information about medical or health conditions, including whether or not you have a disability for which Medecon Healthcare needs to make reasonable adjustments;
- Details of trade union membership; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

7.2 Medecon Healthcare collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving license; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

7.3 In some cases, Medecon Healthcare collects personal data about you from third parties, such as references supplied by former employers, information from employment

background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

8. Adequate, Relevant and Non- Excessive Processing

8.1 If we collect Personal Data directly from Data Subjects, it will only be:

(a) Used for the purpose or purposes as set out in our Privacy Policy or as permitted by the GDPR;

(b) Processed as set out in our Privacy Policy or as permitted by the GDPR; and

(c) Disclosed to the third parties set out in our Privacy Policy or as permitted by the GDPR.

8.2 If we receive Personal Data about a Data Subject from other sources, we will provide the Data Subject with this information as soon as possible thereafter.

8.3 Medecon Healthcare needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

8.4 In some cases, Medecon Healthcare needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

8.5 In other cases, Medecon Healthcare has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows Medecon Healthcare to:

- Run recruitment and promotion processes;
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- Operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;

- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that Medecon Healthcare complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- Ensure effective general HR and business administration;
- Provide references on request for current or former employees;
- Respond to and defend against legal claims; and
- Maintain and promote equality in the workplace.

8.6 Where Medecon Healthcare relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

8.7 Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

8.8 Where Medecon Healthcare processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that Medecon Healthcare uses for these purposes is anonymized or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

9. Accurate Data

We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Not kept longer than necessary for the purpose

10.1 We will not keep Personal Data longer than is necessary for the use or provision of the Services and/or the purpose or purposes for which they were collected. The DPO will perform periodic reviews of retained data against the collection schedule.

10.2 Personal Data will only be retained for the period reasonably necessary to perform the Services and to fulfil the purposes as set out in our Privacy Policy. For example, we will retain Personal Data of Data Subjects whilst they continue to use or contribute to providing the Services and for a reasonable period thereafter, as detailed in the Schedule, unless a longer retention period is required or permitted by law.

11. Data protection impact assessment

11.1 In the event new Processing activities are introduced or we develop new technologies into our business, an assessment of the impact of the change in operations on the protection of such Personal Data shall be carried out in order to address any Processing operations that present a high risk to the rights and freedoms of the Data Subjects or risk non-compliance with the GDPR.

11.2 Such assessment will be carried out with the advice of the Data Protection Officer.

12. Records of Processing activities

12.1 We shall maintain a record of the Processing activities which we carry out. The record will contain the following information:

(a) the name and contact details of the Data Controller.

(b) purpose of the Processing.

(c) description of the categories of Data Subjects and categories of Personal Data.

(d) the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations and the documentation of suitable safeguards concerning this disclosure.

(e) Time limits of erasure of the different categories of data.

13. Processing in Line with Data Subject's Rights

13.1 We will Process all Personal Data in line with Data Subjects' rights, in particular their right, in certain circumstances, to:

(a) Request access to any data held about them by a Data Controller in a commonly used and machine-readable format.

(b) Transmit their data to another Data Controller (free of charge), where such Personal Data is Processed on the basis of consent or contractual performance, unless in doing so, it would adversely affect the rights or freedoms of other Data Subject's or others e.g. including trade secrets or intellectual property.

(c) Prevent the Processing of their data or withdraw their consent at any time in certain circumstances.

(d) Ask to have inaccurate data amended.

(e) Erasure of their Personal Data where data is no longer required for the original purpose or where the Data Subject has withdrawn their consent and no other lawful Processing grounds apply.

(f) Object to the Processing of their Personal Data in certain circumstances.

(g) Lodge a complaint to a supervisory authority such as the Information Commissioner's Office in the UK.

(h) Be notified where their Personal Data is subject to automated decision making i.e. Profiling, including the logic involved, as well as the significance and the envisaged consequence of such Processing for the Data Subject and object to such Profiling in certain circumstances.

(i) Invoke binding arbitration to resolve complaints not resolved by other means.

13.2 Where we are required to provide a copy of Personal Data this will be a free charge, however, any further copies requested may be subject to reasonable fee based on administration costs.

13.3 Where we stop Processing Personal Data or delete a Data Subject's Personal Data, it will possibly mean that that particular Data Subject is unable to continue using or contributing to the provision of some of our Services, and they shall be notified accordingly.

13.4 Where a Data Subject requests to rectify or erase their Personal Data or restrict any Processing of such Personal Data, we may be required to notify, certain third parties to whom such Personal Data has been disclosed of such request.

14. Data Security

14.1 The following policy describes how Medecon Healthcare handles personal data within its organization and the key data privacy principles which it complies with. This section focuses on Medecon Healthcare's role as a data controller and does not form part of Medecon Healthcare's data processing addendum.

14.2 Medecon Healthcare has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer as described in Appendix A ("Security Controls", throughout the entire chain of processing activities by Medecon Healthcare and its sub-processors. Additionally, the Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments.

14.3 Medecon Healthcare takes the security of your data seriously. Medecon Healthcare has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

14.4 Where Medecon Healthcare engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

14.5 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) **Confidentiality** means that only people who are authorized to use the data can access it.

(b) **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorized users should be able to access the data if they need it for authorized purposes. Personal Data should therefore be stored in authoritative data repositories.

14.6 Security procedures include:

(a) **Physical security controls.** Medecon Healthcare facilities feature controls (e.g., alarms, visitor escort process, and access control badges) to prevent unauthorized access.

(b) **Secure lockable desks and cupboards.** Desks and cupboards are required to be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents are shredded and digital storage media are physically destroyed or securely overwritten when they are no longer required.

(d) **Equipment.** Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock the session when it is left unattended.

(e) **Incident Management.** Medecon Healthcare maintains security incident management policies and procedures. Medecon Healthcare notifies impacted Data Subjects without undue delay of any unauthorized disclosure of their respective Personal Data by Medecon Healthcare or its agents of which Medecon Healthcare becomes aware to the extent required by Data Protection Laws and Regulations.

(f) **Technical safeguards.** Medecon Healthcare ensures that technical and organizational measures are in place to ensure data security and minimization, this includes anti-virus, intrusion detection, user authentication services, pseudonymization and encryption of data where appropriate.

15. Transferring Personal Data to a Country Outside the EEA

15.1 We may transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country (or organization) to which the Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms (e.g. based on adequacy decisions, approved binding corporate rules, standard contractual clauses).

(b) The Data Subject has given his or her consent.

(c) The transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defense of legal claims.

(e) The transfer is authorized by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

15.2 Subject to the requirements in paragraph 15.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the Processing of payment details and the provision of support services.

16. Disclosure and Sharing of Personal Information

16.1 Subject to paragraph 15, we may share Personal Data we hold with any member of our suppliers and any subsidiaries as defined in section 1159 of the UK Companies Act 2006.

16.2 We may also disclose Personal Data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose Personal Data we hold to the prospective seller or buyer of such business or assets on a need to know basis.

(b) If we or substantially all of our assets are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets.

(c) If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

16.3 We may also share Personal Data we hold with selected third parties, including but not limited to our business partners, service providers and sub-contractors for the performance of any contract we enter into with them or a Data Subject when we have notified the Data Subjects accordingly.

16.4 Disclosing/sharing Personal Data outside of our organization carries further risks and we must ensure the right organizational, technical and contractual measures are in place before transferring or allowing access to Personal Data.

17. Subject Access Requests

17.1 Under GDPR, data subjects have a number of rights to access, rectify, erase, and restrict processing of Personal Data. These rights include:

(a) access and obtain a copy of your data on request;

(b) require Medecon Healthcare to change incorrect or incomplete data;

(c) require Medecon Healthcare to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;

(d) object to the processing of your data where Medecon Healthcare is relying on its legitimate interests as the legal ground for processing; and

(e) ask Medecon Healthcare to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Medecon Healthcare's legitimate grounds for processing data.

17.2 Data Subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the data protection officer immediately.

17.3 Our employees will refer a request to the data protection officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

17.4 All Data Subject Access requests must be dealt with within a month of receiving them and no Data Subject shall be charged for making such request.

17.5 We will not charge Data Subject Access requests unless any requests which we receive are made excessively, repetitive or are manifestly unfounded requests, we may charge them an administration fee in order to Process such requests or refuse to act on such requests.

18. Reporting Breaches

18.1 Where there has been a Personal Data breach and the breach is likely to result in a high risk to the rights and freedoms of the Data Subject we will report the breach to the Information Commissioner's Office without undue delay and, where feasible, not later than 72 hours after having become aware of it.

18.2 Where there has been a Personal Data breach and the breach is likely to result in a high risk to the rights and freedoms of the Data Subject we will report the breach to the Data Subject without undue delay. The communication to the Data Subject will describe the nature of the Personal Data breach as well as recommendations for the Data Subject concerned to mitigate potential adverse effects. Such communications to Data Subjects will be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with Data Subjects whereas the need to implement appropriate measures against continuing or similar Personal Data breaches may justify more time for communication.

19. Document Control

This Policy needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in business activities, which will or could possibly affect the current operation of the Medecon Healthcare Information Security Management System, and the relevance of this document
- A change in the manner in which Medecon Healthcare manages or operates its information assets and/or their supporting assets, which may affect the accuracy of this document
- An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident, formal review or an audit finding.

The current version of this Policy shall be recorded below.

REVISION HISTORY			
AUTHOR	DATE	VERSION	DESCRIPTION
David Jones	07 May 2018	1.0	Initial revision for Medecon Healthcare
David Jones	03 May 2019	2.0	Yearly Review and agreed by management

REVIEWED AND APPROVED FOR USE BY			
APPROVED BY	DATE	VERSION	SIGNATURE
Zaheer Ali, Senior Management	07 May 2018	1	Approved
Zaheer Ali, Senior Management	03 May 2019	2	Approved By Email
DOCUMENT DISTRIBUTION			
NAME		RESPONSIBILITY	
All Employees including Contractors and Temporary Staff		DPO	

Appendix A: Data Processor Security Controls

1. Nature and Purpose of Processing

1.1 Medecon Healthcare will Process Personal Data as necessary to perform the Medecon Healthcare services and as further instructed by the Customer in its use of the Services, as a Data Controller. This shall include automated processing of Personal Data to evaluate and analyze certain personal aspects relating to the Data Subject, in particular to analyze or predict aspects concerning that Data Subject's personal preference, interests, behavior and location.

2. Categories of Data Subjects

2.1 Customer may submit Personal Data to the Medecon Healthcare services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons);
- Employees or contact persons of Customer's prospects, customers, business partners and vendors;
- Employees, agents, advisors, freelancers of Customer (who are natural persons);
- Customer's users authorized by Customer to use the Services.

3. Type of Personal Data

3.1 Customer may submit, or allow collection of, Personal Data in the use of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name;
- Title;
- Position;
- Employer;

- Contact information (company, email, phone, physical business address);
- ID data;
- Behavioral and profile data;
- Personal preferences;
- Connection data;
- Location data.

4. Data Segregation

4.1 The Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data storage and access based on business needs. The architecture provides an effective logical data separation for different Customers via Customer-specific unique IDs and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

5. Security Controls

5.1 Medecon Healthcare has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer, throughout the entire chain of processing activities by Medecon Healthcare and its sub-processors. Additionally, the Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments.

5.2 Medecon Healthcare adopts a number of security controls, which include:

- Unique user identifiers to allow user to assign unique credentials and assign and manage associated permissions and entitlements;
- Controls to ensure initial passwords must be reset on first use;
- Controls to limit password re-use;
- Password length and complexity requirements;
- Customers have the option to integrate Single Sign-On technologies to directly control the authentication and credential complexity, expiration, account lockout, etc.;

- Customers have the option to manage their application users, define roles, and apply permissions
- User passwords are stored using a salted hash format and are not transmitted unencrypted;
- User access log entries will be maintained.
- If there is suspicion of inappropriate access to any of the information system platform, Medecon Healthcare can immediately block the access and take necessary steps to prevent any unauthorized access.
- User access logs will be stored in a secure centralized host to prevent tampering;
- User access logs will be kept for a minimum of 90 days;
- Medecon Healthcare personnel will not set a defined password for a user.

6. Intrusion Detection

6.1 Medecon Healthcare, or an authorized independent third party, will monitor the Services for unauthorized intrusions using network-based intrusion detection mechanisms.

7. Security Logs

7.1 All Medecon Healthcare systems used in the provision of the Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to facilitate security reviews and analysis.

8. Incident Management

8.1 Medecon Healthcare maintains security incident management policies and procedures. Medecon Healthcare notifies impacted Customers without undue delay of any unauthorized disclosure of their respective Customer Data by Medecon Healthcare or its agents of which Medecon Healthcare becomes aware to the extent required by Data Protection Laws and Regulations.

9. User Authentication

9.1 Access to the Services requires a valid user ID and password combination (or via integrated Single Sign-On mechanism), which are encrypted via TLS while in transmission, as well as machine specific information for identity validation as described under “Security Controls,” above. Following a successful authentication, a random session ID is generated and stored in the user’s browser to preserve and track session state.

10. Physical Security

10.1 Production data centers used to provide the Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around the- clock guards, two-factor access screening, including biometrics, and escort- controlled access, and are also supported by on-site back-up generators in the event of a power failure.

11. Personnel Security

11.1 Medecon Healthcare employment offers are contingent upon successful completion of criminal background and reference checks. Upon commencing employment, all Medecon Healthcare employees receive information security training and are contractually committed to confidentiality clauses to ensure that they adhere to Medecon Healthcare's commitment to security and confidentiality for its customers. Medecon Healthcare’s information security awareness and training program requires employees complete annual security refresher training.

12 Reliability and Backup

12.1 All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Services is stored on a redundant fault-tolerant infrastructure that is replicated to the secondary data center hourly. Data centers forming a regional pair are geographically located in different areas to minimize the possibility of a pandemic or natural disaster impacting both at the same time.

13. Disaster Recovery

13.1 The Services and production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage. The Services' disaster recovery plans currently have at least the following standard target recovery objectives: (a) restoration of the Services (RTO) within 1-3 hours after Medecon Healthcare's declaration of a disaster; and (b) maximum Customer Data loss (RPO) of 1-2 hours; excluding, however, a disaster or multiple disasters causing the compromise of multiple data centers at the same time, and excluding development and test bed environments, such as the sandbox service.

14. Viruses

14.1 The Services have controls in place that are designed to prevent and detect the introduction of viruses to the Services' respective platforms.

15. Data Encryption

15.1 The Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a Customer's network and the Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Any data that is collected and persisted by ONE is encrypted at rest using 256-bit AES encryption. Encryption keys and secrets are safeguarded in a secure data vault that is restricted to authorized users and applications as defined in our access control policy.

16. Change Management

16.1 Medecon Healthcare's Change Management processes are aligned to ITIL to ensure standardized methods and procedures are used to maximize value while minimizing risk of incidents and disruptions when making changes to the Services. The Change Advisory Board reviews all changes for business and security impacts prior to authorizing a change.

16.2 All business systems are provisioned with secure configurations derived from industry best practices and are managed in accordance with Medecon Healthcare's asset management and information classification controls.

17. Access Control

17.1 Medecon Healthcare will not access or modify data except where necessary as directed by Customers to provide the Services or resolve or prevent errors. Access to production data centers is restricted on a per-user basis in accordance with the concept of least privilege and secured using a two-factor authentication enabled VPN that is only accessible via secure management servers.

18. Patch Management

18.1 Patch installation is prioritised based on the severity of the patch with respect to the systems. For example, patches related to critical security issues are given the highest priority and are applied within 48 hours or less.

19. Return of Customer Data

19.1 During the contract term, Customers may export a copy of Customer Data processed by the Services. Within 30 days of termination of the applicable Service, Customers may: 1) request return of Customer Data submitted to the Services; or 2) access their account to export or download Customer Data submitted to Services.

20. Deletion of Customer Data

20.1 After termination of the Service, following the 30-day period for return of Customer Data, Customer Data submitted to the Services is retained in inactive status for up to 30 days, after which it is securely overwritten or deleted.

21. Usage and Trend Reporting

21.1 Medecon Healthcare may track and analyze the usage of the Services for purposes of security and helping Medecon Healthcare improve both the Services and the user experience in using the Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve service functionality.

21.2 Medecon Healthcare may share anonymous usage data with Medecon Healthcare's service providers for the purpose of helping Medecon Healthcare in such tracking, analysis and improvements. Additionally, Medecon Healthcare may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our Services.

22. Sub-processors

22.1 Medecon Healthcare and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities.

22.2 Medecon Healthcare utilizes the services of the following sub-processors to provide part of the Medecon Healthcare infrastructure to host Customer Data and provide the Services:

23. European specific provisions – Overseas Transfers

23.1 The GDPR requires that Personal Data must not be transferred to a country or territory outside the European Economic Area (i.e. the member states of the EU plus Iceland, Liechtenstein and Norway), unless that country or territory or organization ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

23.2 Subject to paragraph 3.20, where the Customer entity and the Medecon Healthcare entity are based inside the EEA, Medecon Healthcare shall not transfer Personal Data to any country outside of the EEA without prior written consent from the Customer, except for transfers to and from: (i) any country which has a valid adequacy decision from the European Commission; or (ii) any organization which ensures an adequate level of protection in accordance with the applicable Data Protection Laws and Regulations.

23.3 Medecon Healthcare complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Medecon Healthcare has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

23.4 The Federal Trade Commission has jurisdiction over Medecon Healthcare's compliance with the Privacy Shield. In certain situations, we may be required to disclose personal information requested by government authorities, including for national security or law enforcement purposes.

23.5 Medecon Healthcare commits to cooperate with The UK Information Commissioner's Office and/or the Swiss Federal Data Protection and Information Commissioner and comply with the advice given by UK Information Commissioner's Office and the Swiss Federal Data Protection and Information Commissioner with regard to personal data transferred from the EU, EEA and Switzerland.

23.6 In the event Medecon Healthcare transfers personal data covered by this Privacy Policy to a third party acting as a controller, Medecon Healthcare will do so consistent with any notice provided to the subjects of that data and any consent they have given, and only if the third party has given Medecon Healthcare contractual assurances that it will (i) process the personal data for limited and specified purposes consistent with any consent provided by the subjects of such data; (ii) provide at least the same level of protection as is required by the Privacy Shield Principles and notify us if it makes a determination that it cannot do so; and (iii) cease processing of the personal data or take other reasonable and appropriate steps to remediate if it makes such a determination. If Medecon Healthcare has knowledge that a third party acting as a controller is processing personal data covered by this Privacy Policy in a way that is contrary to the Privacy Shield Principles, Medecon Healthcare will take reasonable steps to prevent or stop such processing.

23.7 With respect to Medecon Healthcare agents, Medecon Healthcare will only transfer the personal data covered by this Privacy Policy needed for an agent to deliver to Medecon Healthcare the requested product or service. In addition, Medecon Healthcare will (i) permit the agent to process such personal data only for limited and specified purposes; (ii) require the agent to provide at least the same level of privacy protection as is required by the Privacy Shield Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively Processes the Personal Data transferred in a manner consistent with Medecon Healthcare obligations under the Privacy Shield Principles; and (iv) require the agent to notify Medecon Healthcare if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shied Principles. Upon receiving notice from an agent that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles, Medecon Healthcare will take reasonable and appropriate steps to stop and remediate unauthorized processing.

23.8 Medecon Healthcare remains liable under the Privacy Shield Principles if an agent processes personal data covered by this Privacy Policy in a manner inconsistent with the Privacy Shield Principles, except where Medecon Healthcare is not responsible for the event giving rise to the damage.

24. Services Specific Provisions

24.1 Where the Customer has entered into an agreement with specific requirement, Personal Data may be shared with suppliers in relation to the provision of the Medecon Healthcare Services and the relevant to the procured service which the Customer has purchased in the relevant agreement.

25. Confidential Information

25.1 Medecon Healthcare will keep Confidential Information (which of course extends beyond Personal Data) it receives confidential in accordance with the relevant agreement between the Customer and Medecon Healthcare and, except with the prior written consent of the Customer or as permitted in the relevant agreement, will:

- Not use or exploit the Confidential Information in any way except for the purposes for which it has been disclosed;
- Not disclose or make available the Confidential Information in whole or in part to any third party; and
- Apply the technical and organizational measures as detailed in to this Policy to Confidential Information.