Data Protection, Retention and IT Security Policy

Last Modified March 15, 2019

Introduction

This data retention policy sets out the obligations of **OperationsAlly** ("us/we/our/Company") and the basis upon which we protect, store, retain, review and destroy data held by us, or within our custody or control.

This policy applies to our entire organisation including our officers, employees, agents and sub-contractors.

Data Protection Policy

Section A: Overview

1. **The reason for this policy**
   - 1.1 You have legal rights with regard to the way your personal data is handled.
   - 1.2 In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties, and therefore in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.
   - 1.3 All people working in or with our business are obliged to comply with this policy when processing personal data.
2. **Introduction**
   - 2.1 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, for example, customers and business contacts, or that is provided to us by data subjects or other sources.
   - 2.2 It also sets out our polices in relation to data protection
     - a) In general we seek to meet the standards set forth under the General Data Protection Regulation ("the **Regulation**" or "**GDPR**"), however as OperationsAlly is not based within the European Union and does not explicitly market to people living in those countries not every part of the regulation is applicable.
   - 2.3 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.
   - 2.4 The procedures and principles set out herein must be followed at all times by us and our employees, agents, contractors, or other parties working on behalf of the Company.

2.5 We aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

3. The meaning of key Data Protection terms

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data. A data subject is a person on planet earth. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified 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 behaviour.

3.4 **Data controllers** are the people who or organisations 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 Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4. Summary of the Data Protection Principles

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

a) **(Processed fairly and lawfully)** processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) **(Processed for limited purposes and in an appropriate way)** collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) **(Adequate, relevant and not excessive for the purpose)** adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

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

e) **(Not kept longer than necessary for the purpose)** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may

be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) **(Processing in line with data subject's rights)** personal data must be processed in line with data subjects' rights, in particular your right to:

4.2.1 request access to any data held about them by a Data Controller (see also clause 15).

4.2.2 prevent the processing of their data for direct-marketing purposes.

4.2.3 ask to have inaccurate data amended (see also clause 9).

4.2.4 prevent processing that is likely to cause damage or distress to themselves or anyone else.

g) **(Security)** 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.

h) **(Transfers)** note that The Company stores data with third-party companies that are around the globe. We have vetted our vendors and their data security and privacy polices.

5. **Our use of personal data and our purpose**

We collect, hold, and process the personal data referred to in Schedule 1 (and the purpose for which we process that personal data is also set out in Schedule 1).

6. **Our data protection measures**

When we are working with personal data we take **t**he measures set out in Schedule 2.

Section B: Data Protection Principles

7. **Lawful, Fair, and Transparent Data Processing**

The Regulation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The processing of personal data is lawful if one (or more) of the following applies:

a) **(consent)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) **(contract)** processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) **(legal obligation)** processing is necessary for compliance with a legal obligation to which the Data Controller is subject;

d) **(protection)** processing is necessary to protect the vital interests of the data subject or of another natural person;

e) **(public interest)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority

vested in the Data Controller;

f) **(legitimate interests)** processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

8. **Processed for Specified, Explicit and Legitimate Purposes**

8.1 The Company collects and processes the personal data set out in Schedule 1 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and can include data received from third parties.

8.2 The Company only processes personal data for the specific purposes set out in Schedule 1 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

9. **Adequate, Relevant and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 5, above.

10. **Accuracy of Data and Keeping Data Up To Date**

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. **Timely Processing**

The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

12. **Secure Processing**

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

12.1 An assessment of the risks posed to individual data subjects; and

12.2 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

Section C: Data Subject Rights

13. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

d) The right to erasure (also known as the 'right to be forgotten');

e) The right to restrict processing;

f) The right to data portability;

g) The right to object;

h) Rights with respect to automated decision-making and profiling.

14. Keeping Data Subjects Informed

14.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected, specifically within the Privacy Policy and Terms of Use:

a) Details of the Company

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Schedule 1 of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

g) Details of the data subject's rights under the Regulation;

h) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

k) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

14.2 The information set out above in Part 14.1 shall be provided to the data subject at the following applicable time:

14.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

14.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c) In any event, not more than one month after the time at which the Company obtains the personal data.

15. Data Subject Access

15.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

15.2 All subject access requests received must be forwarded to **customercare@operations-ally.com** .

15.3 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. Rectification of Personal Data

16.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

17. Erasure of Personal Data

17.1 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest

to allow the Company to continue doing so) (see Part 20 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation;

17.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

17.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

18. Restriction of Personal Data Processing

18.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

18.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

19. Data Portability

19.1 **The Company processes personal data using automated means. This includes transferring information from one third-party software to another using computer software.**

19.2 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other Data Controllers, e.g. other organisations).

19.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format: PDF and JPEG.

19.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another Data Controller.

19.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

20. **Objections to Personal Data Processing**

20.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).

20.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

20.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

21. **Automated Decision-Making**

21.1 In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

21.2 The right described in Part 21.1 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;

b) The decision is authorised by law; or

c) The data subject has given their explicit consent.

22. **Profiling**

Where the Company uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

Section D: Our Other Obligations

23. **Accountability**

23.1 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the Company and any applicable third party Data Controllers;

b) The purposes for which the Company processes personal data;

c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data from the Company;

e) Details of how long personal data will be retained by the Company; and

f) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

24. **Privacy Impact Assessments**

The Company shall carry out Privacy Impact Assessments when it sees fit. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

24.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

24.2 Details of the legitimate interests being pursued by the Company;

24.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

25. **Organisational Measures**

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

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other

parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;

i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

26. Transferring Personal Data to a Country Outside the EEA

26.1 The Company is not located within the EEA, Clients shall assume that all data collected by the Company is not held within the EEA.

27. Data Breach Notification

27.1 All personal data breaches must be reported immediately to the Company via customercare@operations-ally.com.

27.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

27.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

27.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

28. Implementation of Policy

28.1 This Policy shall be deemed effective as of **May 24, 2018.** No part of this

Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Schedule 1: Our Use Of Personal Data And Our Purpose

The following personal data may be collected, held, and processed by the Company:

a) **Meeting Information, including but not limited to, attendees, scheduling, notes and recordings**

b) **Project and/or Project Deliverables, including but not limited to documents, spreadsheets, presentations, templates and videos**

c) **Shared Documents**

d) **Invoicing and Billing information**

e) **Client surveys and information required to complete projects and/or programs.**

Schedule 2: Our Specific Data Protection Measures

These are the measures we take when working with personal data:

a) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted.

b) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

c) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

d) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

e) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient;

f) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from customercare@operations-ally.com.

g) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

h) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of customercare@operations-ally.com;

i) Personal data must be handled with care at all times and should not

be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

j) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

k) No personal data should be stored in local storage eon any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise.

l) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

m) All personal data stored electronically should be backed up with backups stored **in the cloud**. All backups should be encrypted;

n) All electronic copies of personal data should be stored securely using passwords and data encryption;

o) All passwords used to protect personal data must contain a combination of uppercase and lowercase letters, numbers, and symbols**.**;

p) Under no circumstances should any Company account passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

Data Retention Policy

Objectives

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- our own servers;
- any third party servers;
- potential email accounts;
- desktops;
- employee-owned devices (BYOD);
- potential backup storage; and/or
- our paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The period of retention only commences when the record is closed.

In general we seek to meet the standards set forth under the General Data Protection Regulation ("the **Regulation**"), however as OperationsAlly is not based within the European Union and does not explicitly market to people living in those countries not every part of the regulation is applicable.

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data and how we aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

1. processed lawfully, fairly, and in a transparent manner in relation to the data subject;
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 purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public

interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

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.

The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed.

Security and Storage

All data and records are stored securely via Cloud Services to avoid misuse or loss. We will process all personal data we hold in accordance with our IT Security Policy.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is agreement by them to comply with those procedures and policies, or if there are adequate measures in place.

Examples of our storage facilities are as follows: Dropbox, Google Drive

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 authorised 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 authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the cloud services instead of individual PC's

Retention Policy

Data retention is defined as the retention of data for a specific period of time and for back up purposes.

We shall not keep any personal data longer than necessary, but acknowledge that this will be dependent on the different types of documents and data that we have responsibility for. As such, our general data retention period shall be indefinite, unless there is a request to delete the dat.

From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

Destruction and Disposal

At request, we shall delete confidential or sensitive records categorised as requiring high protection and very high protection, and we shall either delete or anonymise less important documents.

We are responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential records may be destroyed by recycling.

IT Security Policy

1. Introduction

This document sets out the measures to be taken by all employees of **OperationsAlly** (the "Company") and by the Company as a whole in order to protect the Company's computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate or accidental.

2. Key Principles

2.1 In general we seek to meet the standards set forth under the General Data Protection Regulation ("the **Regulation**" or "**GDPR**"), however as OperationsAlly is not based within the European Union and does not explicitly market to people living in those countries not every part of the regulation is applicable.

2.2 All IT Systems are to be protected against unauthorised access.

2.3 All IT Systems are to be used only in compliance with relevant Company Policies.

2.4 All data stored on IT Systems are to be managed securely in compliance with all relevant parts of the Regulation and all other laws governing data protection whether now or in the future in force.

2.5 All employees of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

2.6 All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.

2.7 All IT Systems are to be installed, maintained, serviced, repaired and upgraded by the hired or contracted Information Technology Professionals (the "IT Department") or by such third party/parties as the IT Department may from time to time authorise.

2.8 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity and confidentiality of that data) lies with the IT Department unless expressly stated otherwise.

2.9 All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the IT Department.

2.10 All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the IT Department.

3. IT Department Responsibilities

3.1 The IT Department shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements;

b) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, by way of periodic audits and risk assessments, with regular reports being made to the Company's internal senior management on the condition of the Company's information security and compliance with this Policy;

c) ensuring organisational management and dedicated staff responsible for the development, implementation and maintenance of this Policy;

d) carrying out vulnerability assessments and patch management by using threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code; and

e) ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations and other relevant rules whether now or in the future in force including, but not limited to, CASL, the GDPR and the Computer Misuse Act 1990.

3.2 The IT Department shall be responsible for the following:

a) assisting all Users in understanding and complying with this Policy;

b) providing all Users with appropriate support and training in IT security matters and use of IT Systems;

c) ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities and any special security requirements;

d) receiving and handling all reports relating to IT security matters and taking appropriate action in response;

e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

f) monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future;

g) ensuring all data is being backed up on a regular basis

4. Users' Responsibilities

4.1 All Users must comply with all relevant parts of this Policy at all times when using the IT Systems.

4.2 All Users must use the IT Systems only within the bounds of English law and must not use the IT Systems for any purpose or activity which is likely to contravene any English law whether now or in the future in force.

4.3 Users must immediately inform the IT Department of any and all security concerns relating to the IT Systems.

4.4 Users must immediately inform the IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.

4.5 Any and all deliberate or negligent breaches of this Policy by Users will be

handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

5.1 All software in use on the IT Systems (including, but not limited to, operating systems and individual software applications) will be kept up-to-date and any and all relevant software updates, patches, fixes and other intermediate releases will be applied at the sole discretion of the IT Department. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release and thus falls within the remit of new software procurement and outside the scope of this provision.

5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.

5.3 No Users may install any software of their own, whether that software is supplied on physical media (e.g. DVD-Rom) or whether it is downloaded, without the approval of the IT Department. Any software belonging to Users must be approved by the IT Department and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

5.4 All software will be installed onto the IT Systems by the IT Department unless an individual User is given written permission to do so by the IT Department. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. Anti-Virus Security Measures

6.1 Most IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall and internet security software. All such anti-virus, firewall and internet security software will be kept up-to-date with the latest software updates and definitions.

6.2 All IT Systems protected by anti-virus software will be subject to a full system scan frequently.

6.3 All storage media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be **by the User**.

6.4 Users shall be permitted (and encouraged) to transfer files using cloud storage systems.

6.5 Any files being sent to third parties outside the Company, whether by email, on physical media or by other means (e.g. FTP or shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate.

6.6 Where any virus is detected by a User this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall

promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided **as soon as possible** to limit disruption to the User.

6.7 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

7. Hardware Security Measures

7.1 Wherever practical, IT Systems will be in the cloud, but if on-site, they will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised individual access to such locations for any reason.

7.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment and network infrastructure) and any other areas where personal data may be stored (eg. data centre or server room facilities) shall be designed to (i) protect information and physical assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of the relevant facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

7.3 No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the IT Department. Under normal circumstances whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Department.

7.4 All non-mobile devices (including, but not limited to, desktop computers, workstations and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

7.5 All mobile devices (including, but not limited to, laptops, netbooks, tablets, PDAs and mobile telephones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight.

7.6 The IT Department shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled and the corresponding data shall

be kept on the asset register.

8. Access Security

8.1 All IT Systems (and in particular mobile devices including, but not limited to, laptops, netbooks, tablets, PDAs and mobile telephones) shall be protected with a secure password or such other form of secure log-in system as the IT Department may deem appropriate. Such alternative forms of secure log-in may include fingerprint identification and facial recognition.

8.2 Logical access controls designed to manage electronic access to data and IT System functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all Users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

8.3 All passwords must, where the software, computer or device allows:

8.3.1 be at least **6** characters long;

8.3.2 contain a combination of **letters, numbers and special characters**

8.3.3 not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.);

8.3.4 be created by individual Users; and

8.4 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone including the IT Department and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password they should change their password immediately

8.5 If a User forgets their password, they should take steps to update the password via means provided. If this is not possible, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

8.6 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after **at most 3 hours** of inactivity. This time period can be changed by Users however, Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).

8.7 The IT Department shall conduct regular system audits or event logging and related monitoring procedures to proactively record User access and activity on the IT Systems for routine review.

8.8 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Department. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the IT Department.

8.9 **Users may connect their own devices (including, but not limited to, mobile telephones, tablets and laptops) to the Company network subject to the approval of the IT Department. Any and all instructions and requirements provided by the IT Department governing the use of Users' own devices when connected to the Company network must be followed at all times. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to the Company network or to any other part of the IT Systems. The IT Department shall reserve the right to request the immediate disconnection of any such devices without notice.**

9. Data Protection

9.1 See our Specific Data Protection Policies above.

10. Internet and Email Use

10.1 All Users shall be subject to, and must comply with, the provisions of the Company's Communications, Email and Internet Policy when using the IT Systems.

10.2 Where provisions in this Policy require any additional steps to be taken to ensure IT security when using the internet or email over and above the requirements imposed by the Communications, Email and Internet Policy, Users must take such steps as required.

11. Reporting IT Security Breaches

11.1 All concerns, questions, suspected breaches or known breaches shall be referred immediately to customercare@operations-ally.com

11.2 Upon receiving a question or notification of a breach, the IT Department shall, assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the IT Department deems necessary to respond to the issue.

11.3 Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the IT Department. Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the IT Department.

11.4 All IT security breaches, whether remedied by the IT Department or by a User under the IT Department's direction, shall be fully documented.

12. Business Continuity

12.1 The Company shall state its in place adequate business resiliency/continuity and disaster recovery policy within its Terms of Use and make every attempt to maintain any information and the supply of any service and/or recovery from foreseeable emergency situations or disasters.

13. Severability

13.1 If any one or more of the terms or provisions of this Privacy Policy is deemed unlawful, void or for any reason unenforceable by any court in any jurisdiction, then any such term(s) or provision(s) shall be deemed severable from the remaining terms or provisions in such jurisdiction and will not affect the validity and enforceability of such remaining terms or provisions.

14. Implementation of Policy

This Policy shall be deemed effective as of May 24, 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.