# GENERAL DATA PROTECTION REGULATION (GDPR) AND DATA SECURITY POLICY

**How does Alterline comply with the GDPR principles when processing personal data?**

This document outlines how Alterline complies with the General Data Protection Regulation (GDPR) principles when:

1. processing personal data for research purposes
2. processing personal data for the purposes of marketing Alterline's services.

There are six principles that organisations must adhere to in order to comply with the GDPR when processing personal data.

This policy mentions data subjects, personal data, data controllers and data processors. Where these are mentioned, the terms are defined as:

**Data subject:** a living individual to whom personal data relates.

**Personal data:** any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including, for example: name, email address, phone number, address, identification number, location data or online identifier. This could include chronologically ordered sets of records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. Personal data can also include demographic data or anything else that can be used to identify an individual if responses are specific enough to identify an individual, alone or when combined with other data.

**Data controller:** person or organisation who determines the purposes and means of processing personal data in connection with its own business activities.

**Data processor:** person or organisation who is responsible for processing personal data on behalf of a data controller.

**(1.0) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.**

**Processing for research purposes**

Alterline processes personal data on some occasions as the data controller and on other occasions as the data processor (please see the table below).

***Table 1***

| | Alterline processes personal data as the… | Alterline's client is the… |
|---|---|---|
| Processing personal data for research purposes on behalf of one other organisation (an Alterline client) where the data subjects are 'customers' of, and personal data has been obtained from, that Alterline client | Data processor | Data controller |
| Processing personal data for research purposes on behalf of one other organisation (an Alterline client) where the data subjects are **not** 'customers' of, and the personal data has **not** been obtained from, that Alterline client | Data controller | N/A – personal data will not be shared |
| Processing personal data for research purposes for multiple clients (in one collaborative project) where the data subjects are either 'customers' or are not 'customers' of those Alterline clients | Data controller | N/A - personal data will not be shared |

Where Alterline acts as a third-party data processor on the instruction of a client (data controller), as in the first line of table 1, it is the data controller's responsibility to ensure that the GDPR is complied with and there is a data

processing agreement in place. Alterline provides data processing services to third-party data controllers in compliance with the GDPR.

When processing personal data both as the data controller or as the data processor, Alterline always identifies a lawful basis for processing the data.

Where personal data is collected by Alterline for research purposes (as in lines 2 and 3 of table 1), it is always collected and processed with informed consent as the lawful basis for processing. Informed consent is always transparent, ensuring the data subject is fully informed before they take part in the research about what, how and where their data will be used before they begin to give their data. Informed consent is always collected by way of an affirmative action such as selecting 'next' to continue with a survey, a recorded verbal agreement when taking part in an in-depth interview, or an agreement in writing indicating that they would like to proceed with the research. Data is not processed in any way which is incompatible with the information given when the data subject gave their informed consent. Where we ask data subjects for sensitive data - defined by the GDPR as: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation - Alterline's condition for processing such special category data is the data subject giving explicit informed consent to the processing of that personal data for one or more specified purposes. Alterline collects this type of data only where necessary. Alterline informs data subjects why we are asking for their sensitive data and what it will be used for; data is not processed in any way which is inconsistent with the information which was given when data subjects gave their explicit informed consent. Data subjects are also given the option to tick 'prefer not to say' to any questions that ask for sensitive data.

Where personal data has been shared with Alterline by a third party for research purposes, and Alterline is acting as the data processor (as in line 1 of table 1), we process that data under the lawful basis of 'legitimate interest'. It is within Alterline's legitimate interest to receive personal data from our clients to invite data subjects to take part in independent research on behalf of our clients, as this is Alterline's core business and purpose. If research is not conducted independently, results of the research could be affected by a bias that does not allow respondents to be honest and open. The data controller must identify its own lawful basis for sharing the personal data with Alterline and ensure a data processing agreement is in place for Alterline to process that data. Where a data controller shares personal data with Alterline, we will process only personal data that has been shared securely and lawfully according to the GDPR. If we collect further data linked to the shared personal data, we always do so under the lawful basis of informed consent.

**Processing for marketing purposes**

The personal data that Alterline processes for direct marketing purposes contains only business contacts. This includes generic company contacts (e.g. info@companyname.co.uk), which are not covered by the GDPR, or specific employees of companies and other corporate bodies (e.g. name@companyname.co.uk), which are covered by the GDPR.

The lawful basis for processing this personal data is 'legitimate interest'. It is within the legitimate interest of Alterline to market our products and services to business contacts who work in the sectors that we conduct independent research for, to sell our services as a business. Consent is not needed to process personal data that are in the form of business contacts; however, Alterline always includes a way for specific business contacts to unsubscribe from receiving direct marketing, should they wish. Processing of business contacts in this way is necessary in order for Alterline to tell potential customers/clients about our products/services. Other non-direct marketing methods would not be sufficient alone to allow businesses to become aware of the services that we offer. Business contacts are likely to reasonably expect

that they may be contacted by companies that can provide them with a service which is relevant to the sector/role they work in and can benefit them in some way, and hence be contacted by Alterline by direct marketing about our independent research services. This type of processing is not likely to have a significant impact on the individual personally as it is done in a business context. All GDPR principles and e-privacy laws are complied with when Alterline send direct marketing.

**(1.1) The rights of data subjects**

**(1.1.1) The right to be informed**

**Processing for research purposes**

The processing of personal data for research purposes by Alterline is transparent. Where we are collecting personal data from data subjects, they are always informed of or have access to the following information in order to make sure they are provided with their individual rights and are fully informed about the data which Alterline is or will be processing about them. Personal data is not processed in any way that is incompatible with that about which they have been informed, without further consent.

Before taking part in research, data subjects are informed:

- Who Alterline is, and the contact details of an Alterline researcher related to the research being conducted;
- What Alterline is asking them to take part in and give Alterline their data for; who the data is being collected for; why we are collecting the data; what the data will be used for; and the lawful basis for processing their personal data;
- If Alterline is contacting people as a third-party data processor whose data has been shared with Alterline, we inform the data subject which organisation has shared their data with Alterline, along with their contact details. In this case we inform them why their data has been shared and what we are using it for;
- That Alterline complies with the GDPR, and a link to Alterline's full GDPR policy is provided;
- Alterline does not keep personal data for longer than is necessary for the purposes for which it is being collected. As a minimum, Alterline reviews whether it is necessary to keep personal data one year after data is collected, and deletes any personal data which it is not necessary to keep;
- If the data subject's personal data may be shared with a third-party data processor, data subjects will be informed;
- That they have a right to lodge a complaint with the data controller (an Alterline researcher if Alterline is the data controller, or Alterline's client if Alterline is the data processor – contact details are provided) and, if they are still not satisfied, with the Information Commissioner, should they wish, using the Information Commissioner helpline: 0303 123 1113.

In situations when we are conducting research with anyone under the age of 13, we always obtain parents' or guardians' consent.

The information that we supply about the processing of personal data is concise, transparent, intelligible and easily accessible; it is written in clear and plain language.

**Processing for marketing purposes**

On all direct marketing to named business contacts, Alterline provides instructions on how to opt out of receiving direct marketing from Alterline and a record is kept (a suppression list) of people who have opted out, which new contacts are screened against. Alterline also always identifies who we are, and we give our contact information. All direct marketing informs the data subject of the reason for which they are being contacted and Alterline processes their personal data and has a link to Alterline's GDPR policy.

**(1.1.2) The right of access**

**Processing for research and marketing purposes**

For data of which Alterline is the data controller, data subjects have a right to request access to any information that Alterline holds about them if it is linked to their personal data in any way. If Alterline receives a subject access request, it is Alterline's policy to record the request, respond within two weeks and provide the data to the individual within one month, to comply with the GDPR standards. However, Alterline strives to respond to requests and provide information as soon as possible, which tends to be sooner than the GDPR standard. The identity of the individual is confirmed before personal data is shared, by asking data subjects to confirm at least two pieces of personal information that we hold (or one if only one piece is held). If data that is held is no longer personally identifiable in any way, then subject access requests may be denied. If data subjects request access to data of which Alterline is the data processor, we will inform the data controller and it will deal with the subject access request. Alterline will share relevant personal data that we hold with the data controller to comply with the request.

**(1.1.3) The right to rectification**

For personal data of which Alterline is the data controller, data subjects have a right for their data to be rectified if they believe it is inaccurate or incomplete. If Alterline receives a request to rectify personal data from an individual who we hold data about, it is Alterline's policy to record the request, respond to that request within two weeks and make the rectification within one month, to comply with the GDPR standards. However, Alterline strives to respond to rectification requests as soon as possible, which tends to be sooner than the GDPR standard. The identity of the individual is confirmed before personal data is rectified, by asking data subjects to confirm at least two pieces of personal information that we hold (or one if only one piece is held). If data that is held is no longer personally identifiable in any way, then rectification requests may be denied. If data subjects request rectification to data of which Alterline is the data processor, we will inform the data controller and it will deal with the request. Alterline will rectify data at the request of the data controller.

**(1.1.4) The right to erasure, the right to object and the right to restrict processing**

For personal data of which Alterline is the data controller, data subjects have a right to object to the processing of their personal data and/or withdraw their consent to their data being processed at any point. This can include asking Alterline to erase any personal data that we hold, restrict processing of that personal data, or object to a type of processing that Alterline is completing where the data has been collected with consent or legitimate interest as the lawful basis for processing. There are only certain conditions where an organisation is obliged to erase personal data at the request of data subjects. However, as Alterline only processes personal data with consent or legitimate interest as the lawful basis and the data subject's request for erasure is more important than Alterline's legitimate interest to conduct research, Alterline will always comply with the erasure request where we are the data controller. Data subjects are given details of how to withdraw their consent and or request any of the above. If a request for erasure, an objection or a request to restrict processing is received by Alterline, it is Alterline's policy to record the request, respond to that request within one week where necessary (responses will not be made to straightforward unsubscribe requests) and ensure the request is dealt with within two weeks. Alterline strives to respond to these requests as soon as possible. If Alterline have made personal data which is requested to be erased, publicly available, we will erase this where possible. Alterline will also ask any third party who the personal data has been shared with to erase the requested personal data. If data that is held is no longer personally identifiable in any way, then requests may be denied. If a request for erasure is made, this also involves erasing data from our suppression lists which does mean that subjects are at risk of being contacted in the future if their data is received by Alterline at a later data by other means. If data subjects object or withdraw their

consent to Alterline processing data of which we are the data processor, we will cease communication with the data subject and inform the data controller. We will then act upon the request at the instruction of the data controller.

**(2.0) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.**
**Processing for research and marketing purposes**
Alterline always specifies in an explicit and transparent manner the reason data subjects' personal data is being processed (see section 1.1.1 'The right to be informed'). Alterline is specific and 'granular' about how and why personal data is being processed. The data is not processed further in any way that is incompatible with those purposes without the explicit informed consent of the individual.

**(3.0) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**
**Processing for research and marketing purposes**
Alterline holds only data which is necessary for the purposes which it is processed. Where we collect sensitive data, data subjects are told why it is necessary to collect this data and given the option to answer, 'prefer not to say' (see section 1.0 for more information). Alterline does not keep personal data longer than is necessary and anonymises data where possible, securely deleting personal data associated with it, at the earliest possible point. As a minimum, Alterline reviews whether it is necessary to keep personal data one year after data is collected and deletes any personal data that it is not necessary to keep.

**(4.0) Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.**
**Processing for research and marketing purposes**
All data subjects have the right to rectification if they believe their data to be inaccurate or incomplete. If we receive a request to rectify personal data, it is Alterline's policy to respond to that request within two weeks and for rectification to be made within one month, to comply with the GDPR standards. However, Alterline strives to respond to rectification requests as soon as possible, which tends to be sooner than the GDPR standard. If data which is held is no longer personally identifiable then rectification requests may be denied.

**(5.0) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.**
**Processing for research**
Alterline does not keep personal data longer than is necessary and where possible anonymises data and deletes personal data associated with it at the earliest possible point. As a minimum, we review whether it is necessary to keep personal data one year after data is collected and delete any personal data which it is not necessary to keep. Third-party clients or data subjects must inform Alterline if they feel it is necessary for the personal data to be kept for longer. However, the decision to keep or delete data is made by Alterline. Personal data may be held for longer than a year if it is deemed necessary. Anonymised research data which is not personally identifiable in any way may be kept for longer and does not fall under this principle.

**Processing for marketing purposes**
Data kept for the purposes of marketing Alterline services is often kept for longer than a year. However, a review will still be conducted at yearly intervals on whether it is necessary to keep the data.

**(6.0) Personal data shall be 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.**

NB: The following section is about processing for research and marketing purposes unless otherwise stated.

**(6.1) Software**
If Alterline use any software that will have access to personal data for research purposes, we will inform the data subject(s) of the software being used and provide a link to the software's GDPR/privacy/data protection/security policy. Alterline will always ensure that the organisations running the software comply with the GDPR.

**(6.1.1) Axcrypt**
Alterline uses Axcrypt to encrypt single files.

Axcrypt uses AES-128 encryption. To find out more about Axcrypt security, please click the following link:
https://www.axcrypt.net/information/security/

**(6.1.2) Veracrypt**
Alterline uses Veracrypt to encrypt folders.

VeraCrypt uses AES with 14 rounds and a 256-bit key. To find out more about Axcrypt security, please click the following link:
https://www.veracrypt.fr/en/Documentation.html

**(6.1.3) Snap Surveys**
**Processing for research purposes**
Alterline uses Snap Surveys software to conduct its online web surveys and statistical data analysis. Snap WebHost is the online questionnaire delivery, analysis and reporting service and is operated by Snap Surveys.

Snap Surveys is independently audited and certified by Bureau Veritas as being compliant with ISO 27001, which is the internationally recognised gold standard for information security systems. Security levels are maintained for the service itself, for the platform it is running on, and for the backup and support services behind it. The security package comprises:

- ISO/IEC 27001
- SAS 70/SSAE 16 certified data centres
- Secure (https/SSL), encrypted questionnaire and report delivery
- Data encrypted at rest
- Permanent malware scanning
- Latest security updates applied
- Daily vulnerability scan
- Daily backups
- Optional questionnaire login ID/password
- Enforced password policy for survey management

Our survey data is hosted on Snap Surveys' customer server. Snap Surveys acts as a data processor and Alterline remains the data controller. It processes Alterline's data only in accordance with Alterline's instructions and permissions. As a data processor, it also agrees to take appropriate technical and organisational measures against unauthorised or unlawful processing of the personal data or its accidental loss, destruction or damage.

Snap Surveys has a global customer base and so has both UK- and US-based data centres, which are hosted at UKFast in the UK and Rackspace in the US. Both are ISO 27001-certified organisations running SAS 70/SSAE 16 certified data centres. Data for its UK customers (including Alterline) is stored in the UK data centre and accessed only by UK staff - therefore Alterline data is not transferred outside of the EEA when using Snap Surveys.

In the extremely unlikely event that the main and back-up UK-based servers went down, Snap Surveys would seek express permission from Alterline to transfer data to its US-based server and Alterline would consult with the client if data is being collected on behalf of a third party before any permission would be granted to do this. Please note that this is an extremely unlikely occurrence which we do not envisage will happen.

Snap Surveys deletes any data from their servers a maximum of 14 weeks after Alterline deletes data from Snap Surveys webhost.

Data is encrypted by Snap Surveys using AES 256 encryption. All data uploads and downloads are carried out using SSL (https). All direct communication with Snap WebHost core service is carried out using SSL (https).

If you would like to read more about Snap Surveys security please go to the following link: http://www.snapsurveys.com/survey-software/security-accessibility-and-professional-outline/

**(6.1.4) Skype**
Alterline sometimes uses Skype to complete online focus groups and in-depth interviews. When we use it for online focus groups we provide participants with account login details and ask them not to give any of their personally identifiable information. For in-depth interviews, they either use their own personal accounts or we provide them with one of ours, though again we ask that they do not type any of their personally identifiable information into the account.

Skype uses the AES (Advanced Encryption Standard*), also known as Rijndael, which is used by the US Government to protect sensitive information, and Skype has for some time always used strong 256-bit encryption. User public keys are certified by the Skype server at login using 1536- or 2048-bit RSA certificates. To find out more about Skype's security, please click the following link: https://support.skype.com/en/faq/FA31/does-skype-use-encryption

**(6.1.5) Web Creator Suite**
Web Community Creator is an online community platform that Alterline sometimes uses to host online discussions and research tasks.

To find out more about Web Community Creator's security and privacy, please click the following links: http://webcreatorsuite.co.uk/home/privacypolicy/

**Processing for marketing purposes**
**(6.1.6) Pipedrive**
Alterline use 'Pipedrive' as a data processor to store our personal data that we use for direct marketing purposes. Pipedrive complies with the GDPR. For more information please click the link below: https://www.pipedrive.com/en/privacy

**(6.1.7) Mailchimp**
Alterline use 'Mailchimp' as a data processor to store our personal data that we use for direct marketing purposes and to send out direct marketing emails. Mailchimp complies with the GDPR. For more information please click the link: https://mailchimp.com/legal/privacy/?_ga=2.259396938.1314038275.1524142435-1053869604.1524142435

**(6.1.8) Dropbox**
Alterline uses Dropbox to:

- Store and share (between employees) anonymised and/or pseudonymised data for research purposes
- Store and share (between employees) personal data for research purposes which is encrypted using Axcrypt
- Store and share (between employees) personal business to business data for marketing purposes which is encrypted using Axcrypt
- Store and share (between employees) other files which do not contain personal data.

*Privacy Shield*
The GDPR states that personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Dropbox complies with the EU-US Privacy Shield Frameworks. Adhering to the Privacy Shield Principles ensures that an organisation provides adequate privacy protection under the GDPR.

You can view Dropbox's privacy shield certificate here: https://www.privacyshield.gov/participant?id=a2zt0000000GnCLAA0&status=Active

Alterline does not store any unencrypted Personal Data on Dropbox. However, Dropbox is covered by the Privacy Shield, which allows us to store personal data on it under the GDPR.

*ISO*

The International Organization for Standardization (ISO) has developed a series of world-class standards for information and societal security to help organisations develop reliable and innovative products and services. Dropbox has certified its data centres, systems, applications, people and processes through a series of audits by an independent third party, the Netherlands-based EY CertifyPoint.

ISO 27001 (Information Security Management): ISO 27001 is recognised as the premier information security management system (ISMS) standard around the world. The standard also leverages the security best practices detailed in ISO 27002. To be worthy of your trust, Dropbox continually and comprehensively manages and improves its physical, technical and legal controls. Their auditor, EY CertifyPoint, maintains its ISO 27001 accreditation from the Raad voor Accreditatie (Dutch Accreditation Council). Follow the link below to view Dropbox's ISO 27001 certificate: https://www.dropbox.com/static/business/resources/dropbox-certificate-iso-27001.pdf

ISO 27017 (Cloud Security): ISO 27017 is a new international standard for cloud security that provides guidelines for security controls applicable to the provision and use of cloud services. Follow the link below to view Dropbox's ISO 27017 certificate: https://www.dropbox.com/static/business/resources/dropbox-certificate-iso-27017.pdf

ISO 27018 (Cloud Privacy and Data Protection): ISO 27018 is an emerging international standard for privacy and data protection that applies to cloud service providers like Dropbox which process personal information on behalf of their customers and provides a basis on which customers can address common regulatory and contractual requirements or questions. Follow the link below to view Dropbox's ISP 27018 certificate: https://www.dropbox.com/static/business/resources/dropbox-certificate-iso-27018.pdf

Some third-party apps with Dropbox integration ask for permission to access Dropbox accounts. We do not give permission to third-party apps on our Dropbox account.

**(6.2) Personal data**

While the measures that Dropbox takes offer good security (Privacy Shield – see section 6.1.8), which allows for the storage of personal data, we take an extra step to ensure that we safeguard the personal data that we process.

**Processing for research purposes**

We add an extra layer of security by anonymising data stored that contains personal information, using a unique pseudonym ID number when it is stored on Dropbox. The personal data is then stored encrypted (using Veracrypt software) on a secure laptop and only data that is pseudonymised using an ID number is stored on Dropbox. The secure laptop is stored in a locked cupboard and is signed in and out for use. All data on the secure laptop is backed up once a week on an encrypted hard drive which is stored off site at all other times. Therefore, in the unlikely event that Dropbox is compromised, personal data is not stored on Dropbox, mitigating the impact of a security breach by loss of data.

Personal data processed for research purposes is downloaded only onto the secure data laptop.

Personal data processed for research purposed as standard is not stored on Dropbox. However, if it needs to be shared between Alterline employees on Dropbox temporarily, it is encrypted using AxCrypt software and then removed and stored back onto the secure laptop at the earliest possible stage.

**Processing for marketing purposes**
Most of our data that we process for direct marketing purposes is stored on Pipedrive or Mailchimp. However, it is sometimes also necessary to store lists on Dropbox. Any lists of personal data that are stored on Dropbox are encrypted using Axcrypt.

**(6.3) Transferring personal data**
Personal data transferred by Alterline externally is always transferred using 'Egress Switch Secure Email and File Transfer'. Egress Switch features comprehensive government- and industry-certified security and authentication, including email and file encryption at rest and in transit, multi-factor authentication, and customisable policy controls. It meets legislative and industry compliance requirements, including the GDPR. Users can stay in control of their information after it has been shared both internally and externally by revoking recipient access, preventing actions such as download and copy/paste, and viewing audit logs. Switch is certified under NCSC Commercial Product Assurance, Common Criteria and ISO 27001:2013.

We ask all third parties that transfer data to Alterline to use the same software when transferring personal data to Alterline. You can use this software for free because you are transferring data to Alterline, which pays for the service (instructions for how to use Egress Switch are provided on request if you need them and have not been sent them).

**(6.4) Data processing agreement**
If Alterline is going to share or receive personal data with a third party, we always ensure that a data processing agreement is signed first.

**(6.5) Alterline employees**

Alterline have an internal training programme to ensure data protection and security, and cyber security, and that the GDPR principles are complied with. All Alterline employees have received training and are regularly refreshed on our GDPR and data protection and security policy.

When an employee ceases to work at Alterline, they are locked out of any accounts they have access to, by either disabling accounts or changing passwords.

**(6.6) Antivirus software**
Alterline has full working antivirus software on all its digital devices which contain or have access to personal data.

**(6.7) Secure deletion**
Any personal data that is deleted digitally is erased securely using a secure digital data shredder.

Any hard copy or paper document that contains personal data is stored in a secure locked cupboard. Paper copies of personal details are used only if absolutely necessary. If these can be scanned/photographed and stored under encryption digitally, this is done at the earliest possible point with paper copies destroyed/shredded securely.

**(6.8) Passwords**
Alterline stores passwords securely using LastPass software. If passwords are shared internally, they are only shared using LastPass. LastPass stores passwords securely by using 256-bit AES implemented in C++ and JavaScript (for the website) and it exclusively encrypts and decrypts on the local PC. This means that data does not travel over the internet nor does it ever touch LastPass servers - only the encrypted data does. This is the same encryption algorithm that is used by the US Government to protect its top-secret data. For more information on LastPass security, please see the following link:
https://www.lastpass.com/enterprise/security

We regularly update passwords once every 90 days.

If passwords are shared externally, this is done over the phone and always separate to the platform which the password is for or the channel which the platform is being shared by.

Laptops and computers are set to require 'Ctrl Alt Del' where possible before a password for access can be entered. They are also set to revert to screensaver if there is a period of inactivity of five minutes or more, requiring a password to be entered to re-access the device.

All devices that contain personal data require a password to be accessed.

Passwords to accounts containing personal data are not shared between employees at Alterline. However, employees who have responsibility for data security and/or directors have access to all passwords.

**(6.9) Sharing personal data with third-party data processors**
Before sharing personal data with a third party, Alterline completes the relevant checks to ensure that the third party complies with the GDPR. Alterline also identifies a lawful basis for transferring that data. Before sharing the data, Alterline and the third-party sign Alterline's data processing agreement.

**(6.10) USBs and external hard drives**
USBs and external hard drives are used for personal data only when absolutely necessary. If any personal data is added to an external hard drive or USB which is not the designated encrypted secure data back-up, Alterline employees log what has been added, the date it is added, why it is added and the date it is securely deleted. Personal data will be added only if it is encrypted using Veracrypt or Axcrypt. A log is always made to confirm when the data has been erased and the erasure is always done securely (see section 6.7 'secure deletion'). USBs and external hard drives are stored in a locked cupboard when not in use and a log is made when one is removed and returned.

**(7.0) The controller shall be responsible for, and be able to demonstrate, compliance with the principles.**
This policy demonstrates how Alterline complies with the GDPR principles for its research and marketing practices.

Alterline conducts Data Protection Impact Assessments (DPIAs) for all new processes involving personal data that are likely to result in a high risk to individuals' interests.

Alterline conducts Legitimate Interest Assessments (LIAs) for any process for which legitimate interest is used as the lawful basis for processing.

Regular data protection audits are conducted every six months to ensure that Alterline's GDPR policies are being adhered to. Alterline has an audit process which is followed, and the results of these audits are logged.

**(7.1) Personal data breach**
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. According to the Information Commissioner, examples can include:

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

Alterline has a breach reporting procedure instruction document, which involves reporting a breach to a data protection lead, logging the breach and informing the Information Commissioner's Office and the affected individuals where necessary.

If a personal data breach occurs, Alterline establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then we notify the Information Commissioner's Office and the

individual; if it is unlikely then we log the breach along with the decision not to report it.

Alterline reports personal data breaches to the Information Commissioner within 72 hours of becoming aware of the breach, where necessary and feasible, using the Information Commissioner 's Office helpline number: 0303 123 1113.

## GDPR policy review details

Alterline has the right to update this policy at any point. It will be reviewed every six months as a minimum. The policy will always be kept up to date on the Alterline website.

Date of last policy review: 14/05/2018
Reviewed by: Laura Hotchkiss – Data Protection Lead

Please use the following details to contact Alterline's Data Protection Lead or Managing Director:
Data Protection Lead contact details: Laura.Hotchkiss@alterline.co.uk
Managing Director contact details: Nick.Carley@alterline.co.uk
0161 605 0862

NB: The Data Protection Lead is not a Data Protection Officer.