

## Privacy Policy for Research Participants

### 1.1 Identity and contact details of the data controller

---

Alterline processes personal data on some occasions as the data controller and on other occasions as the data processor. The introduction to the specific research task that you are taking part in will always identify whether Alterline is the data controller or the data processor of your personal data. If Alterline is the data processor, it will identify the identity and contact details of the data controller.

#### **Alterline's identity and contact details**

Name: Alterline Research Limited

Company registration number: 7426250

Manchester address: Flint Glass Works, 64 Jersey Street, Manchester, M4 6JW

London address: Technopark, 90 London Road, London, SE1 6LN

Telephone number: 0161 605 0862

Managing Director: Nick Carley

Managing Director email address: [nick.carley@alterline.co.uk](mailto:nick.carley@alterline.co.uk)

Data protection lead: Laura Hotchkiss

Data protection lead email address: [laura.hotchkiss@alterline.co.uk](mailto:laura.hotchkiss@alterline.co.uk)

NB: The data protection lead is not a data protection officer.

### 1.2 Purpose of the data processing and the lawful basis for the processing

---

#### **Processing purpose**

Alterline processes personal data for the purpose of conducting independent market and social research.

This is most often on behalf of another/other organisation(s), when they have a need for their research to be conducted independently. However, on occasion Alterline also conducts its own research.

Conducting research independently reduces the risk of the results of the research being affected by a bias that does not allow respondents to be honest and open. Alterline may also conduct research on behalf of another organisation because we have specific research expertise or resource that the other organisation may not hold to conduct the research sufficiently.

#### **Lawful basis for the processing**

**Consent:** Where personal data is collected by Alterline for research purposes, 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. This information is always available in the introduction to the research task before you take part. 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 you would like to proceed with the research. Data is not processed in any way that 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 this 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 that 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.

**Legitimate interest:** Where personal data has been shared with Alterline by a data controller for research purposes, and Alterline is acting as the data processor, 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. This lawful basis is always given in the introduction to the research task that you take part in. 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 Alterline collects further data linked to the shared personal data, we always do so under the lawful basis of informed consent.

### 1.3 Categories of personal data

---

Through our research, Alterline may collect the following types of personal data:

- Name
- Email address
- Telephone number
- ID/Membership number
- Postcode
- Demographics

This personal data may be linked to your responses to our research questions, which may include but are not limited to: experiences, perceptions, behaviours and attitudes. However, your responses will not be linked to your personal data when reported unless we get specific consent from you to do this. Your responses may be linked to your demographic details when reported, but we will take our best action to ensure that these demographics do not make you identifiable.

### 1.4 Who will personal data be shared with?

---

Information that you provide will not be associated with your name, identity or contact details when reported. Anonymised information and raw data may be shared with the organisation that the research is being conducted on behalf of (please see the introduction to the research task which you are completing), including demographic information if you provide it, and/or used in research reports that may or may not be available to the public. If you give open-ended responses, quotes from these responses may be used alongside broad demographic information in reports and raw data sets.

Alterline may share your data with a GDPR-compliant third-party data processor for research purposes, though only for the purposes of this research. If Alterline is going to share personal data with a third-party data processor, we always ensure that a data processing agreement is signed first, which means your data cannot be used for anything outside the purposes of the project that you consented for it to be collected for, and that we have a lawful basis for transferring the data to the third party.

If you disclose any information during this research that leads Alterline to believe that you are at risk of harm to yourself or others, we have a safeguarding obligation to report this to the appropriate authority.

Details of third-party software providers that we may store your personal data on or using include:

### 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/>

### 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>

### Snap Surveys

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 that we do not envisage will happen.

Snap Surveys deletes any data from its 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/>

## 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, participants 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>

## 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/>

## 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. Its 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.

### Other software

If Alterline use any software that will have access to personal data for research purposes, we will inform you of the software being used and provide a link to their GDPR/privacy/data protection/security policy. Alterline will always ensure that the organisations running the software comply with the GDPR.

## 1.5 Transfer of personal data to another country

---

Alterline uses only software or third-party data processors that do not transfer personal data outside of the EEA, or that have the Privacy Shield to be compliant with the GDPR and ensure security of your personal data.

## 1.6 Retention period or criteria used to determine the retention period

---

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 which it is not necessary to keep.

## 1.7 The existence of each of data subject's rights

---

### The right to be informed

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 that Alterline is or will be processing about them. Personal data is not processed in any way which is incompatible with that which they have been informed about, 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 acting as a third-party data processor, and is contacting people 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 which the data 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 that 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.

### **The right of access**

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 which 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.

### **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.

### **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. 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 data which 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 date 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.

#### 1.8 The right to lodge a complaint with a supervisory authority

---

You 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 in the introduction to the research task that you are completing) and, if you are still not satisfied, with the Information Commissioner should you wish, using the Information Commissioner helpline: 0303 123 1113.

#### 1.9 The source of the personal data

---

If Alterline has received your personal data from a third party (the data controller) and is acting as a data processor, the introduction to the research task which you are taking part in will always state where we have received your personal data from and the contact details for them.