Privacy Policy for Direct Marketing Recipients

1.1 Identity and contact details of the data controller

Alterline is the data controller for data that we hold for direct marketing purposes. We always identify ourselves and our contact details in any direct marketing that we send.

Alterline's identity and contact details
Name: Alterline Research Limited
Company registration number: 7426250
Manchester address: International House, 61 Mosley Street, Manchester, M2 3HZ
Telephone number: 0161 503 5760
Managing Director: Nick Carley
Managing Director email address: nick.carley@alterline.co.uk
Data protection lead: Zara Lawson (Maternity Cover)
Data protection lead email address: Zara.Lawson@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 direct 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. These contacts may be gathered from information that is in the public domain or may have been given to Alterline by the contacts themselves.

Lawful basis for the processing
Legitimate interest: 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. Business contacts are likely to reasonably expect that they may be contacted by companies who can provide them with a service that is relevant to the sector/role they work in and can benefit them in some way. 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 sends direct marketing.

1.3 Categories of personal data

The personal data that Alterline processes for direct marketing purposes may contain the following fields:

Organisation - Name
Organisation - Address
Organisation - Sector
Organisation - Twitter
Organisation - Website
Organisation - Phone number (switchboard)
Organisation - Number of customers

Organisation - Annual turnover
Person - Name
Person - Phone
Person - Email
Person - Role
Person - Twitter
Person - Job title
Person – LinkedIn

Other information about your relationship with Alterline and/or the projects you are interested in or are involved in may be kept alongside this information.

1.4 Who will personal data be shared with?

Alterline will not share your personal data outside of Alterline unless the information is already available in the public domain.

1.5 Transfer of personal data to another country

Alterline will only transfer personal data outside of the UK using software or third-party data processors under one or more of the following conditions:

a) It is being transferred to a country which is inside the European Economic Area (EEA)

b) It is being transferred to a country for which an 'adequacy decision' has been made

c) Alterline and the receiver have entered into a contract which includes standard data protection clauses adopted by the Commission called a 'Standard Contractual Clause'.

If at least one of the above conditions is not met, Alterline will not transfer personally identifiable data outside of the UK.

Your personal data may be stored on Mailchimp or Pipedrive or encrypted using Microsoft Office password protection on OneDrive. Please see below for information about these.

Pipedrive
Alterline use 'Pipedrive' as a data processor to store the 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

Mailchimp
Alterline use 'Mailchimp' as a data processor to store the 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 below:
https://mailchimp.com/legal/privacy/?_ga=2.259396938.1314038275.1524142435-1053869604.1524142435

OneDrive
Alterline uses OneDrive for Business 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 Microsoft Office password protection

- Store and share (between employees) personal business to business data for marketing purposes which is encrypted using Microsoft Office password protection
- Store and share (between employees) other files which do not contain personal data.

Data centres within the EU
OneDrive for Business data centres are located within the EEA for companies whose billing address is in the UK. Therefore, data and files which Alterline store on OneDrive are not transferred outside of the EEA.

For more information click on the following link:

https://learn.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide

Encryption of data in transit

In OneDrive for Business and SharePoint Online, there are two scenarios in which data enters and exits the data centers.

- Client communication with the server: Communication to OneDrive for Business across the Internet uses SSL/TLS connections. All SSL connections are established using 2048-bit keys.
- Data movement between data centers: The primary reason to move data between datacenters is for geo-replication to enable disaster recovery. For instance, SQL Server transaction logs and blob storage deltas travel along this pipe. While this data is already transmitted by using a private network, it is further protected with best-in-class encryption.

For more information click on the following link:

https://learn.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide

Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content. While BitLocker encrypts all data on a disk, per-file encryption goes even further by including a unique encryption key for each file. Further, every update to every file is encrypted using its own encryption key. The keys to the encrypted content are stored in a physically separate location from the content. Every step of this encryption uses Advanced Encryption Standard (AES) with 256-bit keys and is Federal Information Processing Standard (FIPS) 140-2 compliant. The encrypted content is distributed across a number of containers throughout the datacenter, and each container has unique credentials. These credentials are stored in a separate physical location from either the content or the content keys. For more information click on the following link:

https://learn.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide

For more information about how OneDrive safeguard data in the cloud in general, please click the following link:

https://learn.microsoft.com/en-us/sharepoint/safeguarding-your-data

While the measures that OneDrive takes offer good security which allows for the storage of personal data, we take an extra step to ensure that we safeguard the personal data that we process.

Personal data which is stored on OneDrive is encrypted using Microsoft Office in built file password protection options. Microsoft Office uses AES-256 encryption.

1.6 Retention period or criteria used to determine the retention period

Alterline does not keep personal data longer than is necessary. There is no time limit on this for data that we hold for marketing purposes, as it is necessary to keep your personal data as long as you may still have an interest in our products or services. We will erase/amend any personal data that we hold if we are requested to do so by the data subject or we become aware that you are no longer in that role.

1.7 The existence of each of data subject's rights

The right to be informed
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. All new contacts are screened against this list. 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 also has a link to Alterline's GDPR/privacy policy.

The right of access
For data of which Alterline is the data controller, data subjects have a right to request access to any information which 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.

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 to 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 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.

1.8 The right to lodge a complaint with a supervisory authority

You have a right to lodge a complaint with the data controller (Alterline) – please see the contact details in section 1.1 if you would like to make a complaint. If you are still not satisfied, you have a right to contact the Information Commissioner should you wish, using the Information Commissioner helpline: 0303 123 1113.

1.9 Source of the personal data

Personal data held by Alterline for marketing purposes may be gathered from information which is in the public domain or may have been given to Alterline by the contacts themselves. If for any reason Alterline has received from a third party your personal data which is not already in the public domain, we will state where we have received your personal data from.