

Privacy Policy

INTRODUCTION

We respect your privacy and understand that privacy is important to you and that you care about how information about you is used, so this privacy policy sets out details about what data we collect and how we use it.

VISITORS TO OUR WEBSITE

Where we collect personal data via our website, we will be upfront about it and it will be obvious to you that you're providing personal data and how we will be using it.

Google Analytics

When someone visits our website (<http://healthtechalliance.uk>) we make use of the Google Analytics service to collect standard information about visitors to the site and their behaviour (e.g. what pages they viewed). The data provided by Google Analytics is anonymised and in no way enables us to identify individual visitors, however, Google Analytics will place a cookie on your device to enable the service. For more information about how Google Analytics cookies work on websites visit:

<https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>

Other cookies used, tracking pixels or similar tools

We use cookies to:

- remember your acceptance of our cookie banner (when you first visit the website)
- auto-remember your details when you fill out a webform on our site
- Handle anti-spam comments on our posts
- Improve the way we write and promote the content on our website

We also use a number of cookies that are essential to the running of our website.

If we embed content from other websites into our web pages (e.g. videos, images, articles, etc.), the content (including the setting of any cookies or similar tools) behaves in the same way it would if you had visited the content on the other website directly. In such cases, you should check with the original website regarding their use of cookies, their privacy policy and how they may use your data. Whenever possible, we will provide a link to this information.

Online forms

If you fill out one of our website forms (e.g. our “Contact Us” form) a notification email is sent to the relevant team within our company and stored within their email application on their computer. No copy of the data you submit is stored anywhere else. As our site uses SSL (https) the data you submit using the contact form will be encrypted once you press the “submit” button.

Hosting

Our websites are hosted by a third-party hosting provider based within the EU. As such the provider is responsible for maintaining the security of the servers which store the websites, but they do not have any access to our website files. We use SSL to secure the connection when you visit our website, this includes the encryption of data transferred (e.g. data entered in our contact form) to us from the website.

PEOPLE WHO RECEIVE OUR NEWSLETTERS

If you have signed up to receive the Political Intelligence or the Health Tech Alliance email newsletters, or we have added you to one of the email lists (where it is lawful for us to do so) you will receive emails from us via our email list provider. Whilst our email list provider is not based within the EU, we have carried out the necessary checks to ensure they are compliant with EU standards of data protection and are signed up to the Privacy Shield EU-US agreement (as they’re based in the US).

Whenever we send an email to you, using this service, you will always see the option to unsubscribe, should you wish not to receive further emails.

PEOPLE WHO CALL OUR OFFICES

If you contact our offices to discuss working with us, because you’re an existing client or a member of the Health Tech Alliance, depending on your reason for contacting us, we may enter your details in our contacts database. This database is hosted by a third-party provider and whilst our provider is not based within the EU, we have carried out the necessary checks to ensure they are compliant with EU standards of data protection and are signed up to the Privacy Shield EU-US agreement (as they’re based in the US). Your details may also be stored in our email system, particularly if we follow up via email.

PEOPLE WHO CONTACT US VIA EMAIL

If you contact us via email your email will be stored in our email package and on our employee’s computers. We may also download emails or file attachments and store them on our local server (particularly if you’re a customer). We scan all emails for spam and

viruses using a third-party service. Where emails are stored (and scanned) in the cloud, they are done so within the EU.

PEOPLE WHO ATTEND OUR EVENTS

If you attend an event that is organised or co-organised by us, we may enter your details in our contacts database, to enable us to keep you updated about the event, to manage your attendance at the event and, where it is lawful for us to do so, to let you know about other events. This database is hosted by a third-party provider and whilst our provider is not based within the EU, we have carried out the necessary checks to ensure they are compliant with EU standards of data protection and are signed up to the Privacy Shield EU-US agreement (as they're based in the US). Your details may also be stored in our email system, particularly if we follow up via email.

We may share your details with co-organisers and sponsors of our events but will seek your consent before doing this.

OUR USE OF SOCIAL MEDIA

Whilst we may interact with you via social media, we do not collect or store any information other than via the social media platforms.

PEOPLE WHO ARE POLITICAL INTELLIGENCE CUSTOMERS OR MEMBERS OF THE HEALTH TECH ALLIANCE

We will only process the data necessary to maintain our connection with you as a customer or a member of the Health Tech Alliance. This means we will process your data for the purposes of maintaining your contact details (in our customer management system, client database and email service) or via our email lists (as set out above). We may also process your personal data via our timesheet system. We do not process any other information about you.

Our customer management service and timesheet system are third-party cloud-based applications, and whilst our providers are not based within the EU, we have carried out the necessary checks to ensure they are compliant with EU standards of data protection and are signed up to the Privacy Shield EU-US agreement (where they're based in the US).

OUR EMPLOYEES

If you are employed by us, we will maintain the minimal amount of information necessary for maintaining that employment as required by your contract of employment. This will include your name, email address, phone number, next of kin, bank details (for paying you).

Our employee data is stored in a cloud-based service for the purposes of managing payment of your salary.

We may also keep signed paper copies of your contract. These are kept secure and locked away.

RECRUITMENT

If you apply to work with us, we will keep a copy of your CV and associated information on an internal server which is only accessible to our Managers. We will keep this data for up to 6 months in line with our retention policy. Where we print out your application information, we will always ensure it is stored securely and locked away when not being used.

RETENTION

Unless stated elsewhere in this document or in our terms of services we only store the data necessary to provide the services we provide to you, in line with our internal data retention policy. We will keep this data for as long as it is lawful for us to do so (this may be for as long as you are a customer or because of a legal obligation to retain the information, whichever is the longest).

THIRD-PARTY PROCESSORS

We use a number of third-party cloud-based services for the purposes of effectively running our business and providing our services to you. We may also from time to time, use a number of third-party organisations, e.g. accountants, HR support, etc.

In all cases where we are using a third-party service or company, we will only provide the minimal amount of information for the purposes of delivering the service to us and to meet our requirements.

We always carry out due diligence against all our third-party suppliers for the purposes of ensuring their compliance with data protection, maintaining adequate security of your data and ensuring they apply adequate data protection principles to the processing of the data we supply. We also ensure a contract is in place between us and the third-party to ensure data protection compliance at all times.

YOUR RIGHTS

Under current data protection legislation in the UK, you have rights as an individual which you can exercise in relation to the data we store and process about you. You can find more information about your rights on the Information Commissioner's website:
<https://ico.org.uk/for-the-public/>

Complaints

If you want to make a complaint about the way we are processing your data, you can contact us, using the contact details below. You also have the right to complain to the Information Commissioner's Office: <https://ico.org.uk/concerns/>

How to withdraw consent and object to processing

Where we are processing your data and needed to ask your permission to do so, you are able to withdraw your consent at any time. If you wish to stop receiving our marketing emails you can do so, by clicking on the "unsubscribe" link at the bottom of the emails. Otherwise, you can contact us, using the contact details below.

If you wish to raise concerns about the way we are processing your data or would like to raise an objection, then please contact us, using the contact details below, with your concerns.

Keeping your data up to date

It is important that any of your data that we process is kept up to date. We will from time to time ask you to verify your contact details but if you wish to update any information, we hold about you, please contact us using the contact details below.

Erasure of your data (the "right to be forgotten")

Under some circumstances you may request us to delete your data from our systems. Where this is possible (e.g. we don't have any legal purpose for continuing to process your data) we will erase it from our systems.

If you wish to exercise your right to be forgotten, please contact us via the contact details below.

Portability

Your right to portability allows you to request a machine-readable format of the data you supplied to us and associated service logs (where we store them). Please contact us, using the contact details below, if you wish to receive a CSV export of your data.

Access to your data

You have the right to ask us about what data we hold about you, how we process it and provide you with a copy of the data, free of charge and within one month of your request.

To make a request for any personal information we hold and process about you, we would prefer it if you could put it in writing or in an email to the addresses below. We will need to

verify your identity before providing the information and where necessary may contact you further to ensure we understand what data you are requesting.

DISCLOSURE OF INFORMATION

We do not share any personal data with any third parties unless it is lawful for us to do so, if required by law to do so or if you provide us with permission to do so.

MORE INFORMATION

For more information about your data rights and privacy or data protection in general visit the Information Commissioner's Office website: <https://ico.org.uk>

HOW TO CONTACT US

If you have any questions about how we collect and use your information not covered in this privacy policy, or if you wish to speak to someone about our approach to data protection and privacy, please contact:

Till Sommer
69 Wilson St
London EC2A 2BB
contact@political-intelligence.com

CHANGES TO OUR PRIVACY POLICY

We may change or update elements of this privacy policy from time to time or as required by law. The most current version of our privacy policy will always be available via our websites.

1. Document control

Version	Date	Author	Status	Comments
v1	28/10/19	Till Sommer	Final	First version