What are the issues around privacy and confidentiality?

It is quite common for people to have meetings and appointments which they would like to remain private, and they are therefore right to raise concerns about what happens when that private data is handled by Inspirometer.

The headline is that your private data is at least as secure in the Inspirometer system as it is in your own – but what does that mean, and what can you do to ensure that the right things are concealed from the attention of others?

This document looks at these questions from the following perspectives:

- How do you exclude private appointment data from Inspirometer?
- How do you exclude private meeting data from Inspirometer?
- Can you still get feedback on private meetings?
- How can you keep specific agenda items private?
- How secure is data that has been sent to Inspirometer?

How do you exclude private appointment data from Inspirometer?

By default, appointment data (calendar items to which no-one is invited – there is no ‘To’ list) are not included in Inspirometer, and there are no copies of your appointment data on the Inspirometer system.

There are however two exceptions to this:

1. Where the appointment is identified as travel
2. Where the appointment is identified as a meeting

Appointments are identified as travel or meetings by including certain key words within the subject of the appointment. These key words can be found (and can be altered) on your settings page for the Inspirometer add-in (see right).

If you have set up your calendar and key words correctly, there is no reason why confidential appointment subjects should ever appear in your meetings data. In the event that you do want such an appointment to appear in your travel or meetings stats, we would ask you to be circumspect about the subject title you assign to it.
How do you exclude private meeting data from Inspirometer?

Private meetings can be identified to Inspirometer by prefixing the subject of the meeting with one of the privacy identifiers you have included in your Inspirometer settings page (see picture on previous page).

Prefixing your meeting subject with a privacy identifier will cause Inspirometer to replace all occurrences of the subject with Priv:Alias (where Alias is the text which appears before the @ symbol in your email address).

Please note, this only happens within the Inspirometer system – it does not affect any references with your calendar or on your own system.

Can you still get feedback on private meetings?

Prefixing your meeting subject with a privacy identifier does not affect the feedback settings for the meeting – only how its subject name appears within that feedback and within your meeting stats.

If you wish to disable feedback for a meeting (private or otherwise) you have two options: do not include meetings@inspirometer.com in the invite list (you can do this by selecting and deleting it if it has been automatically included from your add-in); or by deselecting the radio buttons on the meetings settings pop-up (providing it is active*) when the meeting is sent.

*see the tick-box under Feedback Options in the picture on the previous page

How can you keep specific agenda items private?

There are a number of options for excluding the titles of specific agenda items from the Inspirometer data (see the example invitation body shown on the right).

In the first example – agenda item 2 – simply omitting the hash from in front of the number will omit this item from feedback, and no record of the item will be stored in the Inspirometer database.

However, if you do want feedback on the confidential item, then the example used for agenda item 3 would be more suitable, where the #numbered item contains an innocuous reference to the agenda item, and any sensitive information is included on the (unhashed and unnumbered) line below. Ensure you put a line break between the two – line wrapping is ignored in Inspirometer.

The results of the above invite are shown on the right.
Essentially, Inspirometer only processes lines that are preceded by a hash and a number, and so if you don’t want certain text to appear in Inspirometer, don’t put it on a line preceded by a hash and a number.

How secure is data that has been sent to Inspirometer?

In respect of the security of meeting invitations (and the data they contain) within the Inspirometer system: The meetings@inspirometer.com calendar is a secure exchange account held within the Microsoft Office365 environment. Office365 implements the oAuth2.0 protocol for access, the specification for which can be found here: [https://tools.ietf.org/html/rfc6749](https://tools.ietf.org/html/rfc6749)

Login for the Meetings@Inspirometer.com calendar via username and password has been disabled, and the account can only be accessed via an oAuth.2.0 Access token. The Access token changes with every access and can only be renewed using a “Refresh Token”. The Refresh Token is renewed each time it is used to get a new Access token. These tokens are cryptographically generated and are over 1000 characters long.

When the Inspirometer system retrieves the Calendar information, it is stored in our dedicated MySQL database within the Microsoft Azure Cloud platform. The database server is only accessible via SSL certificate authentication, using AES256 symmetrical public/private key encryption. Without these keys it is impossible access the server, even for the MySQL Database itself. The Inspirometer system only retrieves the Calendar information it requires to enable feedback and meeting stats. Attachments and the body of the invitation are ignored and do not become part of the Inspirometer database.

The following diagram shows the security of the various parts of the Inspirometer system.
Our Inspirometer servers are running within a virtual environment within the Azure Cloud platform. Please see here for the security in place for their cloud network. Governments and large multinationals trust Azure with their data, here a few of their customers: Apple iCloud; Pixar; Ebay; Travelocity; Boeing; EasyJet; Samsung; Xerox; 3M; NFL; Diebold; NBC; Mazda; GE Healthcare

In other words, your meeting data is more secure on our system than it is on the system and devices of any other invitee to that meeting, including yourself.