

Due diligence and new technologies

Compliance: The New Normal

Background

The use of technology in the workplace to facilitate remote working has surged since the start of 2020, and so has its use in adjusting to the 'new normal' as it relates to business intelligence.

Many of the learnings forced upon us have become opportunities to work faster, better, and provide a better user experience for market research participants, researchers and analysts.

Is it really new?

We recognise that many of our colleagues, whether working for pharma companies, data analytics, market research or fieldwork agencies, or freelance recruiters and personal members, may well be familiar with these technologies. However, it is recommended best practice to assess technology in use at regular intervals, against any new legal or compliance requirements, or any changes to how they operate: including both how they are used in your organisation or what features the solutions offer.

The guidance in this document provides some helpful questions members can ask themselves when assessing new technology and doing their due diligence before using it on live projects.

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. There is no one-size-fits-all approach to the management of risk, and members are encouraged to consult with senior management, their IT department or outsourced vendor, or their organisation's information security policies when assessing how technology will fit into their working practices. Whilst every reasonable effort is made to make sure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA.

Using 'new' technologies

There are as many uses for technology in business intelligence (BI) as there are logistical or business problems that organisations may face in the running of BI activities.

Below are some that are most likely to be familiar or relevant to members. Please consider these uses when reviewing the next sections.

- Electronic signature (e-signature) of consent forms
- Automatic recording transcription software
- File-sharing software
- Tele- or video-conference software


It is not the intention of the BHBIA's Ethics & Compliance Committee to recommend, endorse or otherwise approve a particular solution, platform, or technology over another. Any reference made to a commercial product is for illustration purposes only, and members are encouraged to review the range of solutions available on the marketplace to find the one that will be right for their organisation.


Best practice due diligence questions

Below are some questions we recommend members ask themselves in relation to technology they are considering for use as part of a BI activity.

Privacy by Design

- Is there evidence the solution provider communicates clearly about the privacy implications of their technology, for example in a **relevant privacy policy**, or other documentation?
 - o For example, does their website have a 'Privacy' or 'GDPR' hub you can consult?
- Does the solution provider hold recognised certifications, trust marks, accreditations, or similar **credentials in relation to privacy and data protection**?
 - o For example, are they Cyber Essentials Plus or ISO 27001-certified?
 - o Are they visibly registered with the ICO as Data Controllers?
- Does solution provider's website include or refer to a **dedicated role or professional for privacy**, data protection, compliance, or associated matters?
- Where are all the privacy documents stored and maintained?
- How are the data incidents reported, monitored, investigated and mitigated?
- Does the solution comply with your client's contractual requirements?
- If you have used the solution before, does it provide **clear and concise information to users**, whether or not they are administrators for the platform, **about privacy**?
 - o For example, see below for examples of messages displayed on Microsoft Teams when either starting to record a meeting, or attending a meeting that is recorded.

 **You're recording** You are recording this meeting. Make sure to let everyone know that they are being recorded. [Privacy policy](#)

 **Recording has started.** This meeting is being recorded. By joining, you are giving consent for this meeting to be recorded. [Privacy policy](#)

- Does the solution comply with your client's contractual requirements?
- Has the solution been externally validated by a qualified IT consulting firm as being robust in privacy terms?

Legal framework

You may need to look into or seek advice in relation to the legal status of certain solutions and features they provide, for example, **electronic signatures**.

E-signatures

In the UK, the eIDAS Regulations¹ provide that electronic signatures have legal effect and admissibility in most situations and establishes which signatures cannot be signed electronically and require a “wet” signature. However, some organisations may have policies contrary to this and expect participants to sign and scan hard copy consent forms before taking part in market research activities.

When electronic signatures are to be used for the purpose of BI agreements and/or consent forms, sub-contractors should agree this in advance with their clients, this may be particularly important for international clients where the legal framework may differ from the UK’s.

Security - Encryption

Encryption can be applied to data stored (data at rest) and data as it is transferred (data in motion). Is encryption provided as standard for the solution, or is it a premium feature? It is also good practice to find out the standard of encryption used.

Privacy settings

Consider the following questions:

- What level of control have you got over the solution’s settings? Is there a ‘Trust Centre’ or ‘Privacy Settings’ section you can use to apply restrictions on how the data will be processed? Does the solution offer a graded privacy setting e.g. “high, medium, low” which can be matched to the use-case in mind?
 - o For example, are default settings designed to minimise data processing?
- Does the solution allow you to achieve your objective with minimal processing of personal data, such as allowing ‘first name only’ or allowing initials instead of full names?

Data management

The use of third-party systems or solutions outside of your organisation’s networks introduces additional risks in relation to the management of your processing activities. It is important to be confident about how the solution will store, transfer, back-up, delete any personal data for which you are a data controller or data processor, including where this processing will occur, and by whom.

Retention

Consider the following questions:

- For how long will the solution provider retain personal data they process on your behalf?
- Can you control the retention period applicable to personal data to ensure it is consistent with your internal and contractual requirements, or assurances given to participants?
- Can the maintenance and deletion processes be automated?

¹ The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019) and The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016

- Are these processes logged?
- Does the solution provider offer to automatically clear personal data from files after a set period of time so that it can be retained as pseudonymised data instead?

Note on retention periods: there isn't one appropriate retention period for a type of material or personal data, as individual organisations may be subject to statutory retention periods, specific contractual agreements with their clients, and operational restrictions applicable to the storage and retention of data. Each organisation must determine retention periods that are compatible with their legal and contractual obligations, including not to retain information any longer than necessary. Organisations must make sure they have control over, and can apply a retention policy across, the full range of systems or platforms they will use to process personal data, including third-party systems.

Location

Consider the following questions:

- Where will the personal data be processed or stored, and is this location compatible with the safeguards you have in place for the transfer of personal data?
 - For example, if a non-UK provider, where are the servers based?
 - Can you choose the geography or region in which data will be stored?
 - What information does the solution provider offer in relation to this?
 - If personal data will be processed in a third country², have individuals been notified or has informed consent for this been sought? Are additional safeguards in place?
 - Check with your IT services provider if they have any concerns about cloud based data storage. Also check that hosted solutions can be configured to store your data in appropriate geographic locations.

For more information on the international transfer of data, please read the BHBIA guidance on international transfers available at the following location:

https://www.bhbia.org.uk/assets/Downloads/Guidelines/dp_data_security_aug2020_fv.PDF

Access

Consider the following questions:

- Who has access to the personal data being processed? Can this be controlled? Who can authorise new permissions being granted? How often are access rights reviewed? How well is the password and MFA policy enforced?
- Will the provider or its employees have access to this information? If they do for legitimate purposes, e.g., maintenance, do they commit to doing so only when they absolutely need to?

² For more information about the definition of 'third country', please consult the BHBIA's page on Brexit preparedness (<https://www.bhbia.org.uk/resources/news/preparing-for-brexit-latest-guidance>)

Example 1: File sharing method for lists or recruitment schedules	Example 2: TDI on a teleconference platform	Example 3: Automated transcription software
<p>When sharing data with clients or vendors, it's important we do this securely—can you ensure only authorised recipients of the file will have access?</p> <p>E.g., how does an authorised user authenticate themselves to access the files?</p> <p>Can you restrict access to 'view-only', so they don't need to download, if it isn't necessary for the purpose for which it is being shared?</p> <p>Is access auditable?</p>	<p>Teleconference platforms can make it very easy to inadvertently reveal information about participants.</p> <p>Who can view the personal data of call participants, e.g., e-mail address or full name?</p> <p>When the invitation goes out, does it include all parties in the Cc box or can it be sent so that the identity of other participants/guests is hidden?</p> <p>If the meeting is being recorded, where will the recording be stored and who will have access?</p>	<p>Some providers now offer platforms where the recording is uploaded by the moderator and automatically transcribed, including some teleconference platforms who offer this as a built-in service but...</p> <p>Will anyone from the provider team have access? What does the software do with the audio? Will any human editors have access?</p> <p>Is this information readily available to you if required?</p>

Conclusions

Remember: it's not enough to ask these questions only once, and you should consider documenting your findings when you complete a solution provider assessment.

You should consider scheduling a date to return to this assessment to determine whether you will need to reconsider your solution provider due to:

- a) the introduction of new features,
- b) changes to your legal and contractual obligations,
- c) changes to your organisation's risk appetite,
- d) changes to alternative solutions on the market

There is no denying that technology is here to stay and changes fast, but we need to recognise our responsibilities in making sure our use of new solutions is consistent with our legal obligations and ethical commitments as business intelligence professionals, and asking the right questions is a great place to start.

Prepared by the BHBIA's Ethics & Compliance Committee March 2021

British Healthcare Business Intelligence Association
 Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
 t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales