New technologies: due diligence and online security in Business Intelligence (BI) and Data Analytics (DA)

Compliance: The New Normal

Background

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

Similarly, rapid advances in the potential and realised improvements that technology unlocks for business means that most businesses are constantly on the lookout to deliver better commercial and client outcomes by making appropriate and ambitious use of technology.

This comes with countless opportunities to work faster, smarter, better, and to provide a more optimal user experience for market research participants, researchers and analysts.

However, the regulatory landscape also requires businesses to reflect upon the impact that the use of technology can have on privacy and associated compliance risks – particularly in relation to personal data, special category data, and confidential, proprietary, or sensitive information.

This document is structured as follows:

- How to think about new technologies – What is the scope of this guidance?
- Key risks – What to look out for in your MR/BI activities?
- Due diligence questions – What to look out for when thinking about technology providers?
- Practical tips – Steps you can take to help mitigate your risk

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.

Thinking about "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 and/or AI-led translation and/or transcription software
- File-sharing software
- Tele- or video-conference software

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 or upcoming 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.

Different organisations have different ways of working; therefore, it is important to put this guidance in the right context. Whilst the examples above are likely to apply most frequently, you may need to consider other uses of 'new' technologies not listed above that are relevant to you.

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

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.

Key risks

Remote workers, especially freelancers or small businesses, do not enjoy the same level of IT security infrastructure provided by large corporations or in the traditional bricks and mortar setting. Some common considerations and questions to bear in mind should include:

1. How do we handle data transfers and/or storage?

The use of free document storage and sharing services, e.g. Box, Sharefile, WeTransfer or Google Drive, can carry data protection risks, for example:

- Many free services use cloud-based technology with servers located abroad or in unknown locations, with no control over or the ability to select appropriate data residency regions.
- Free or trial versions tend to offer limited control over data security and retention, for example by not allowing the implementation of a password policy or multi-factor authentication (MFA). These free or trial versions are often limited in time, and do not always make any guarantees as to the retention of your files after the trial period, which may lead to accidental deletion.
- Some data transfer and/or storage solutions also don't automatically include additional security to ensure that only the intended recipient can access the link, by allowing anyone with the link to the folder or file to access it (e.g. even if sent to the wrong person)
- The data held in free, or trial versions may not be subject to any encryption.

2. How do we maintain and demonstrate participant and/or end client anonymity when video conferencing/webcam technology is used?

Different platforms work in different ways, and it's not always clear how to set things up out of the box to preserve the anonymity of participants and clients when setting up a call. Consider:

- Who sends out the invite to the activity and sees contact details.
- How the participant and client join the call, and how their identifiers are displayed to each other, both in the lobby, chat, and as their display icon.
- Whether someone can join the call who wasn't explicitly invited, for example if they were forwarded the invite by someone else on the call, rather than only if authorised by the host.
- Whether observers can be kept out of the call in a waiting area until such time that standard reassurances and introductions have been made with the participant.
- Who has access to recordings made during the call, where they are stored, and whether you need to consider the impact of any AI features like automated transcription or summaries.

3. How do we make sure we capture signatures securely remotely?

In most MR/BI environments, the days of paper forms and wet signatures are truly over. However, you need to consider how to prevent electronic signatures or alternative methods to capture signatures from introducing risks (privacy and otherwise) to your activities.

- Is the form you are using to capture this consent suited to electronic signatures?
- Do you have a process to download and store a copy of the signed document in accordance with your or the client's retention policy and requirements in relation to these documents?
- Who has access to the signed documents and where are these stored?
- Who receives a copy of the signed form for their records, and how?
- If you need to provide the client with copies of signed forms, do you have a method to anonymise a signed PDF and is it well understood across your organisation?

4. How do we ensure confidentiality and security when conducting online MR? And consider the well-being of participants?

- Have you considered what is communicated to participants at recruitment stage?
- How are participants informed about any use of online identifiers and/or other online tracking activity, and what is your legal basis for this processing?
- Does your privacy information reflect your current working practices for online research? Do you have a process to ensure that any changes in your working practices are reflected, if applicable, in any participant-facing communications?

5. When we utilise self-recorded MR or ethnography (i.e., participants audio record and/or film themselves in their own environment), how do we ensure this is done in accordance with the principle of data minimisation? We need to take into account the risk of other individuals being recorded without their consent (accidental intruders).

- Have participants been provided with guidance to minimise this risk?
- Did you consider what would happen to any materials submitted by participants if they include any personal data which was not supposed to be processed?
- Do you have a process to anonymise the materials before they are transferred?

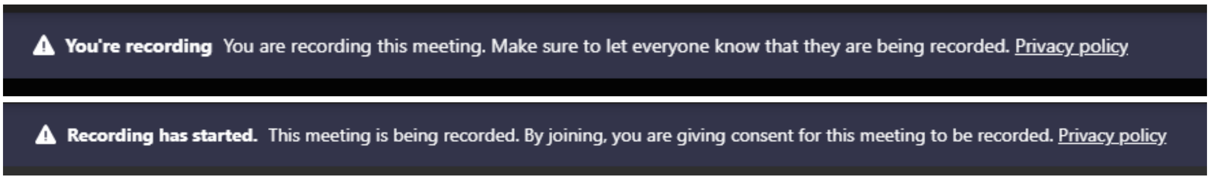
Due diligence questions

To try and effectively address some of the risks we have highlighted above, including any other risks you may identify when assessing your use of technology across your MR/BI activities, we have provided a list of questions that members should be asking of their technology providers (or from their IT teams with responsibility for the sourcing, set up and onboarding of these providers), before deploying these new technologies.

Privacy and security posture of the provider

A key step is to look at any information shared by the provider in relation to their maturity as it relates to privacy by design and by default, information security and data protection.

- Is there evidence the solution provider communicates clearly about the privacy implications of their technology, e.g. in a relevant privacy policy, or other documentation?
    - 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**?
    - Are they Cyber Essentials Plus or ISO 27001-certified?
    - Are they certified to ISO 27701, for Privacy Information Management?
    - Are they visibly registered with the ICO as data protection fee payers?
- Does the 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 any data incidents reported, monitored, investigated and mitigated?
- How will the solution provider assist you in managing any data subject requests?
    - Can you export relevant personal data to respond to a data subject access request (DSAR)? Can you delete or anonymise relevant personal data?
- 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**?
    - 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

- 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 Regulations[1] 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.

Contractual framework

Larger organisations will have legal and procurement teams responsible for the review of contractual agreements in place to cover relevant services to be performed, however small organisations or freelancers may not have the same level of support in place. It is important for all members to consider any general or specific contractual requirements in place as they related to the processing of personal data and/or information security, e.g. where a minimum baseline for information security has been established and agreed with your clients for MR/BI work.

Encryption

You should also consider the extent to which the data stored is encrypted, and to what standard, in line with requirements of the UK GDPR (Art. 32)

[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

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.

Settings

- 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 or data classification scheme e.g. "high, medium, low" which can be matched to the use-case in mind?
    - 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 technology providers 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?
- 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

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 country 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/guidelines-and-legislation/privacy-data

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?
- 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 necessary?

Below is a table with examples of different scenarios and key considerations

Example 1: File sharing method for lists or recruitment schedules	**Example 2**: Tele-depth interview (TDI) on an online platform	**Example 3**: Automated transcription software
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? E.g., how does an authorised user authenticate themselves to access the files? 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? Is access auditable?	Online platforms can make it very easy to inadvertently reveal information about participants. Who can view the personal data of call participants, e.g., e-mail address or full name? 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? If the meeting is being recorded, where will the recording be stored and who will have access?	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… Will anyone from the provider team have access? What does the software do with the audio? Will any human editors have access? Is this information readily available to you if required?

Practical tips

We offer some practical topics below for MR/BI and DA practitioners.

Manage access control

To work effectively as a team, people must have access to shared folders and/or drives, but you should decide and control who has access to what and what level of access is granted. Best practice tells us that users should be granted access based on the least privilege and need-to-know principles. In other words, give users only as much access as they need to perform their role, and nothing more. In addition, access should be revoked at the earliest opportunity.

Make it clear that everyone should keep an eye on this – just because someone suddenly has access to something doesn't automatically mean they can and should access it, either.

You should consider how you revoke any access granted once it is no longer required, including in terms of how you manage project teams, leavers, and keep this under regular review.

Do your due diligence with the software you use

Using the steps we have outlined in this document, ensure you carry out an assessment of platforms, software, or other technology that you may use in your work.

Carry out Data Protection Impact Assessments (DPIAs)

A DPIA can be a helpful way of considering any risks involved in the use of technology on your MR/BI or DA work, even where it is not required by applicable data protection law. You can also use it to document any measures you are taking to protect against or mitigate these risks, so that others can be informed of the steps you've taken and also to keep this under regular review.

When done correctly, a good DPIA can be used like a briefing document to your teams on the appropriate use of technology in the working environment and the starting point of your SOPs.

Write and publish basic Standard Operating Procedures (SOPs)

Technology by its very nature will change quickly, much faster than the legal and regulatory landscape. What was safe and acceptable at a point in time may no longer be appropriate.

Therefore, member organisations are encouraged to write and keep SOPs under review for the use of technology across their MR/BI activities to ensure any solutions are deployed in a consistent and compliant manner, which should account for any updates to these solutions.

Share written guidance with participants

You should consider how the use of technology will impact participants and their ability and/or willingness to comfortably and conveniently take part in MR/BI activities. This may be best served by producing plain English, practical guidance to your participants ahead of or during their participation in MR/BI activities to address any questions or concerns they may have.

Conclusion

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.

Final words

Technology always moves faster than legislation but the principle of lawfulness, fairness and transparency still applies to our practice. Clear, simple and consistent instructions will always help in terms of data protection, security and adherence. Regular reviews, especially if timed to coincide with major technology upgrades will add value.

Further reading

The ICO publishes information for organisations that want to review their IT and data security practices, you can refer to the following hub: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/.

The UK Government's National Cyber Security Centre (NCSC) also publishes some guidance around a variety of topics, see: https://www.ncsc.gov.uk/section/advice-guidance/all-topics.

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.

Prepared by the BHBIA's Ethics & Compliance Committee March 2021 and updated in April 2025 to reflect changes to best practice.

British Healthcare Business Intelligence Association
St James House, Vicar Lane, Sheffield, S1 2EX
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455