Ethics and Compliance Update

September 2019

This update includes:

Guidance from the ICO

Naming the end client

Naming the end client as data controller

There is no further news from the European Data Protection Board (EDPB) or the UK's data protection regulator, the Information Commissioner's Office (ICO) in terms of formal or more detailed guidance upon interpretation of the definition of data controller. We are continuing to work with regulators and government and we will update members when there is news, so please look out for it.

Latest update on naming end clients as data controllers (Oct 2018)

Circumstances when the end client must be named

It is important to remember that there are three independent circumstances in which the end client will have to be named:

1. If the client is the source of personal data that was not obtained from the individual e.g. if they supply a list for sampling (either directly or via a third party list provider) OR
2. If the client receives personal data e.g. they receive non-anonymised video footage of a group discussion OR
3. If the client is a sole or joint data controller determining the purpose and means of data processing.

If you think naming the client at the outset will adversely impact the rigour and robustness of the research then you may be able to name them at the end of the interview.

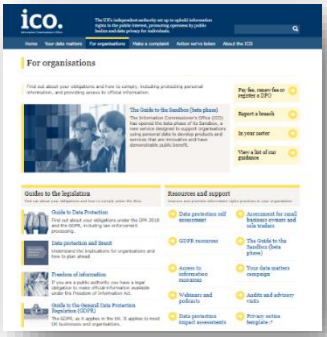
For more detail please go to:

BHBIA's Legal and Ethical Guidelines August 2019, Section E4.2, pages 10-11
https://www.bhbia.org.uk/guidelines-and-legislation/legal-and-ethical-guidelines

Data Protection & Research, Guidance for MRS Members and Company Partners 2019
https://www.mrs.org.uk/pdf/MRS%20Data%20Protection%20and%20Research%20Guidance%20(May%202019)%20.pdf

BHBIA Ethics & Compliance

New guidance from the ICO



The ICO has in recent months provided new guidelines on interpretation of the General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA).

The key requirements are integrated into the BHBIA's Legal and Ethical Guidelines, however if you want more detail we have outlined below what is available from the ICO and where to find it. ICO guidance is user friendly.

Controllers and Processors

This includes checklists to help organisations determine whether they are a controller, a processor or a joint controller and detailed guidance about what it means to be a controller or processor.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Contracts and Liabilities

Whenever a controller uses a processor or a processor uses a sub-processor, there must be a written contract (or other legal act) in place; the GDPR sets out what needs to be included in the contract. This guidance details responsibilities, liabilities and what to include in the contract.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Encryption

The GDPR requires organisations to implement "*appropriate technical and organisational measures*" to ensure secure processing of personal data and includes encryption as an example of an appropriate measure (depending on the nature and risks of your processing activities). This guidance is designed to help organisations to understand the importance of encryption and includes recommendations and practical examples.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/

For further more detailed guidance on encryption go to:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/

Exemptions

In some circumstances, the DPA 2018 provides an exemption from particular GDPR requirements. If an exemption applies, an organisation may not have to comply with all the usual rights and obligations. The exemptions include statistical, scientific or historical research. However the ICO state that "*it does not apply to the processing of personal data*

for commercial research purposes such as market research or customer satisfaction surveys."

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

International Transfers

The GDPR primarily applies to controllers and processors located in the European Economic Area (EEA) with some exceptions. It restricts transfers of personal data outside the EEA, unless the rights of the individuals in respect of their personal data are protected (or one of a limited number of exceptions applies). This guidance discusses the ways in which protected ex-EEA transfers may be made.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a means to help organisations identify and minimise the data protection risks of a project. They must be carried out for processing that is likely to result in a high risk to individuals. The ICO guidance helps you to decide when and how to do a DPIA and includes a template.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Data Sharing

The ICO have produced a draft Data Sharing Code of Practice (Version 1.0 for public consultation 20190715) to provide practical guidance for organisations about sharing personal data in line with data protection law.

https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

Subject Access Requests (SARs)

The ICO's guidance on the time frame within which SARs have to be responded to. Previously SARs had to be responded to within one calendar month, with the day after receipt counting as day 1. This has now changed and day 1 is now the day of receipt e.g. a SAR received on 3 September should now be responded to by 3 October.

Brexit, Data Protection and Business Intelligence

If there is a deal the UK will be subject to EU law and apply the GDPR at least until the end of any transitional period.

If there is no deal at present the UK will be a third country from 31 October 2019. Key data protection consequences of this would be:

- Organisations will need an alternative legal basis for their transfers from the EU to the UK because there would be no more unrestricted transfers of personal data to the UK.
- The ICO will no longer be able to act as lead supervisory authority i.e. the co-ordinating Data Protection Authority for cross-border data processing issues.
- Controllers and processors established in the UK and in the EEA may need to appoint a representative in the EEA and UK respectively.
- Organisations relying on the Privacy Shield for transfers of personal data to the US will need to ensure that the US organisation expressly commits in its privacy notice to applying the Privacy Shield principles to transfers coming from the UK.

Further details on the implications and the BHBIA's recommended actions are available on the BHBIA website in the 'Brexit Implications' guides available through the Privacy & Data Protection web page: https://www.bhbia.org.uk/guidelines-and-legislation/privacy-data

Challenges to Data Transfer Mechanisms

Use of the Privacy Shield and Standard Contractual Clauses

to facilitate the secure transfer of personal data to third countries were challenged in the EU Courts of Justice in July this year.

Judgments in these cases are expected towards the end of 2019 or in early 2020. Either one or both of them could be invalidated as mechanisms for transferring personal data outside the EU - similar to the way in which the Safe Harbor agreement was invalidated in 2015.

If they are invalidated, accessible alternative options are very limited. One potential solution for intra-group transfers is Binding Corporate Rules but getting these approved is time consuming and organisations will probably need an interim solution which regulators are going to have to provide. The BHBIA's Ethics & Compliance Committee will keep you up to date with any developments. For more information about secure overseas data transfers please see the BHBIA's 'Data Security including Breaches and Transfers' available through the Privacy & Data Protection web page: https://www.bhbia.org.uk/guidelines-and-legislation/privacy-data

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters. 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.

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 No: 9244455