

BHBIA Data Analytics Guidelines

Guidance for Analysts Conducting Secondary Data Projects

These guidelines are part of a series designed to provide guidance on the legal and ethical issues impacting data analysts

INTRODUCTION

Secondary market research involves collecting and using data that already exists (for one purpose) and re-using it for another different purpose.

The following is designed to be a check list for those working with secondary data.

DO

Consent

- ✓ Check that you have permission to use the data for your intended purpose under the terms and conditions of the contract or license. If in doubt contact the data owner for permission.
- ✓ If the data are being supplied by a third party, check their terms and conditions. These should set out any limitations on the use of the data, based on the consent given by the original respondents. If there is any doubt, we would recommend contacting the supplier and asking for clarification.
- ✓ If you would like to use personal data from a third party for a reasonable purpose that is not stated within the terms and conditions, contact the supplier and state your request. With some collection mechanisms, such as panels, it may be possible to enhance the privacy terms at the point of collection.
- ✓ Open data (also referred to as Public Access Data) must have a license that it is 'open data', without a license the data cannot be re-used in any way. The license will state the uses that the data may be used for.
- ✓ Reference secondary data appropriately in reports and publications.
- ✓ Whilst the open data license is designed to enable everyone to use the data for the benefit of the wider society, various laws and legislation still apply to open data – copyright laws, database rights, and where personal data is available Data Protection law and Freedom of Information Act 2000 apply.
- ✓ The Open Government License has few restrictions but some do not allow commercial use, so you should check carefully. (See the Open Access Data /Open Sources Guidelines for further information).

Data Protection

- ✓ Refer to Data Protection law (the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018), these detail the requirements for processing data. Be aware that personal data is still protected under data protection law when being used as secondary data.
- ✓ Check whether the source contains 'personal data' (see the BHBlA's Data Analytics Guidelines: *Data Protection and Secondary Data – Key Definitions*). If it does not, data protection law does not apply.
- ✓ Maintain the anonymity, confidentiality and privacy of data subjects by anonymising or pseudo-anonymising the data before secondary use. Only re-use personal data if it's absolutely necessary, with the informed consent of the data subject and in accordance with data protection law.
- ✓ Avoid harming any data subjects through the re-use of their personal data.

Security

- ✓ Keep all secondary data secure; protect it from theft, unintentional use, destruction or damage.
- ✓ Share secondary data only on a need to know basis.
- ✓ Follow all the appropriate data security processes to protect the data.
- ✓ Privacy Impact Assessments (PIA's) are a tool that you can use to identify and reduce the privacy risks of projects. The Information Commissioner's Office (ICO) provides guidance to help organisations decide whether a PIA is necessary. See the ICO's website for further details.

DON'T

- ✗ Don't use or re-use secondary data in any way that would bring you or the healthcare industry into disrepute, reduce confidence or breach laws and regulations.
- ✗ Don't re-use, share or distribute secondary data, especially personal data and sensitive personal data unless you are legally and contractually allowed to do so.
- ✗ Don't transfer secondary data via insecure channels.
- ✗ Do not use personal data in datasets unless they are required. Where records contain personal data, but these data are not important for your purposes, ask the provider to remove the personal data fields before sending you the information. The data is then classed as anonymised and Data Protection law no longer applies to its use.
- ✗ Don't re-use personal data unless it is absolutely necessary and then only in accordance with data protection law.
- ✗ The Open Government License does not cover the use of personal data.

For further information see:

Open Government Licence
<https://data.gov.uk/terms>

The Information Commissioner's Office website
<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/>

The BHBlA's website
<https://www.bhbia.org.uk/guidelines-and-legislation/privacy-data>

Copyright and Database Rights
<https://www.gov.uk/copyright/overview>

This guidance is provided by the BH&IA for information purposes only and is not intended and should not be construed as regulatory or legal advice. It does not cover all legislative and regulatory requirements pertaining to Members and it is the responsibility of all Members to familiarise themselves with these.

The Guidelines are provided by the Data Analytics Guidelines Team within the BH&IA's Ethics & Compliance Committee,

Jason Bryant, Data Analytics Team Lead

Darren Kottler, Data Analytics Team

Klaas Breukel, Data Analytics Team

Catherine Ayland, BH&IA Ethics Advisor

If you have any queries about these Guidelines, please visit www.bhbia.org.uk and submit your query via 'My BH&IA' dashboard. Please note: this ad hoc advisory service is available to full BH&IA members only.

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