BHBIA Data Analytics Guidelines
Data Protection – Basic Do's and Don'ts

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

INTRODUCTION

Most BHBIA members process personal data. If you process personal data make sure you understand what you can and can't do with it!

Also see 'Data Protection – How does the law apply to secondary data?' in the BHBIA's Data Analytics Guidelines series.

DO

✓ Make sure you **understand what 'personal data' is, what 'processing'** personal data means and whether when you process personal data you/your organisation are/is a data controller or a data processor. Your role as controller or processor may change from project to project.
See the BHBIA's Data Analytics Guidelines: *Use of Secondary Data – Key Definitions*

✓ If you process personal data you must **pay a fee to the Information Commissioner's Office**. This applies to every commercial organisation whether you are a large multi-national or a sole trader. Once registered you have to keep your registration up to date so for instance if you change any of the purposes for which you use the data you have to update your notification.

✓ You must:
- Have a specific and legal reason to collect, hold or share personal data
- Not use the data in ways that have unjustified adverse effects on the individuals
- Be transparent about how you intend to use the data, and give appropriate privacy notices
- Handle people's personal data only in ways they would reasonably expect
- Make sure you do not do anything unlawful with the data.

✓ Data controllers must have **written contracts** with processors (e.g. sub-contractors) ensuring the security of the data.

✓ If you require **consent** to process personal data, this consent must be a clear affirmative action, freely given, specific and informed. This means that individuals must be made aware of who will have access to their personal data, for what purpose and any other information that would be required to ensure fair processing. Remember you can only use the personal data for the purposes for which it was collected. Remember also to allow for people wishing to opt out or "the right to be forgotten".

✓ Make sure the personal data is **secure and protected** and that access is limited to those that 'need to know', this will include making sure that:
- Only authorised people can access, alter, disclose or destroy the data
- If the data is lost, altered, destroyed it can be recovered without harm to the individual
- The level of security is appropriate to the nature of the data and to the harm it may cause the individual if lost or stolen

- ✓ **Re-use** of personal data is not prohibited under Data Protection legislation but there are limitations, the re-use purpose must be compatible with the original purpose for which consent for processing was given.

- ✓ Make sure you understand the **terms and conditions** attached to any personal data you want to process - just because you can access it, doesn't make it legal to use it, for instance, many websites only provide data for personal use only, or prohibit commercial use, the copyright or licence may prohibit use of certain types of use.

- ✓ Make sure that when personal data is **transferred** it is protected by law:
  - Make sure the transfer is essential
  - Know exactly which countries it's going to and what this means in terms of restrictions
  - Plan your approach if there are restrictions in place
  - Have contracts in place with all involved parties
  - Export the data securely.

- ✓ Make sure that all those involved in processing personal data **understand their responsibilities** under Data Protection law. This includes making sure the data held is **accurate.**

- ✓ Your company should have a **policy** that deals with data protection issues e.g. amongst many other things, it should tell you what to do if you are asked for a copy of the personal data you hold about them by an individual or what to do if an individual request that the personal data you hold about them is deleted.

DON'T

- × Do not collect personal data unless you have to.

- × Do not collect or hold personal data without a specific and legal reason to do so.

- × Personal data cannot be re-used for a purpose that is incompatible with the original purpose. An incompatible re-use would include one not specified within the privacy notice, it would also include any use outside of what the individual would reasonably expect

- × Do not hold or collect more personal data than is required or justified by the purpose.

- × Do not store personal data for longer than it is needed.

- × Do not export or transfer personal data overseas unless it's essential.

- × Do not keep inaccurate data. Update it or delete it.

For further information see:

The Information Commissioners Office website
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

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

This guidance is provided by the BHBIA 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 BHBIA's Ethics & Compliance Committee,

Jason Bryant, Data Analytics Team Lead
Darren Kottler, Data Analytics Team
Klaas Breukel, Data Analytics Team
Catherine Ayland, BHBIA Ethics Advisor

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