BHBIA Ethics
& Compliance

BHBIA Data Analytics Guidelines
Data Protection – How does the law apply to secondary data?

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

INTRODUCTION

Data Protection law (based upon the General Data Protection regulation (GDPR) and the Data Protection Act (DPA) 2018) sets out the requirements that must be adhered to when processing or controlling ‘personal data’. The guidance below covers the application of data protection law when using secondary data – i.e. data collected by someone other than the user.

Also see ‘Data Protection – Basic Do’s and Don’ts’ in the BHBIA’s Data Analytics Guidelines series.

DO

- ✓ **Check whether the source contains ‘personal data’** (See the BHBIA’s Data Analytics Guidelines: *Data Protection and Secondary Data – Key Definitions*). If it does not, data protection laws do not apply.

- ✓ Be aware that personal data is still protected by data protection law when being used as secondary data.

- ✓ **Purpose - can be problematic if the secondary use was not anticipated** when the data was collected. The original data subjects will have consented to their data being used for one or more purposes - consent is always purpose specific. These constraints remain for the lifetime of the data (and subject) whenever it is in an identifiable form.

- ✓ Where possible, think ahead and ensure that any likely secondary uses of data are considered when gaining consent from data subjects.

- ✓ 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 to enable your request in the future.

- ✓ You must cite a legal basis for the processing of personal data. There are several options available, and which is best will depend on various factors such as your intended use of the data and the length of time you want to hold on to it. Consent, legitimate interest, and contractual obligations are typically the most common legal bases used for secondary data in our context, but only consent is likely to be relevant for special category data, for instance, data about an individual’s health.

- ✓ If you intend to incorporate secondary personal data into systems, you must **check where the data will be held.** Under data protection law, restrictions apply to the countries in which data can be held, and can prohibit storage in most territories outside of the European Economic Area. Increasingly data warehouses are located on cloud servers or in global data hubs, making this a key consideration in today's businesses. Remember, this applies to fail-over sites and backups too.

- ✓ Be aware that data about living individuals recorded in systems such as **CRMs or KAM tools** is also covered under data protection legislation. Ensure you can cite a legal basis for the data you are collecting, minimise the data you collect to that which you need, and issue training regarding the appropriate data to be collected in free text fields (as this becomes primary data and is not covered under the consents collected by your list provider).

- ✓ Store personal data securely, appropriate technical and organisational measures (commensurate with the sensitivity of the data and the risk of harm) are essential to safeguard personal data. Physical (e.g. locked doors) and virtual (e.g. passwords and encryption) security is required as well as virus and perimeter protection (e.g. firewalls).

- ✓ Consider that some exemptions are possible if the data are being used purely for research purposes (scientific, statistical and historic), where the research is not targeted at any particular individuals within the data.

- ✓ There are specific and stringent requirements under data protection law if you are using the Personal Data as part of a fully automated decision making process, which has a direct impact on the data subject. This is known as "Profiling" and more details can be found here.

DON'T

- × 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.

  Note – if you have the personal data anywhere, or can link the data back to a person using other information you hold, the data is still classed as personal.

- × If using personal data for research purposes, do not process or use the data in a manner allowing **decisions targeted at living individual** to be made as this will negate any exemptions that may have applied.

- × Do not use **out of date data where inaccuracies could occur**. Data protection legislation require us to ensure personal data is up to date and adequate for the task it is put to (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/). This can be problematic where secondary data was purchased as a one off in the past.

- × Do not **provide personal data to others** within your organisation without informing them of the purposes for which it can be used, and ensure the security of the data at all times. This will help your colleagues to use the data appropriately.

For further information see:

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

"Preparing for data reform" on the MRS website
https://www.mrs.org.uk/article/mrs/preparing-for-data-reform-gdpr

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

Updated August 2020