BHBIA Data Analytics Guidelines
Data Protection &
Secondary Data Key Definitions

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 you must make sure you understand what you can and can't do with it! To do this you need to understand basic data protection terms.

The terms defined below are not as you might expect presented in alphabetical order, they are presented in a logical sequence leading on from each other.

GENERAL DATA PROTECTION REGULATION (GDPR) & DATA PROTECTION ACT (DPA) 2018

Controls how personal data is used by organisations, businesses or government. To use some of the terms below – the GDPR and the DPA 2018 regulate the processing of personal data across the European Union and the UK respectively, protecting the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers) and those that process the data (data processors). The UK DPA 2018 enacts the GDPR in to UK law.

PERSONAL DATA

Any data relating to an identifiable living person which alone or in combination with other accessible information can identify the individual:

- May be a single piece or series of pieces of data which allow identification of a living individual
- Includes names, addresses, post codes, phone numbers, email addresses
- Alphabetical, numerical, graphical, photographical or acoustic
- Data kept on paper, stored in a computer memory or a video-recording

Personal data includes video-streams (relayed live or delayed and non-anonymised recordings) and may include audio recordings. Whether an audio recording is considered personal data depends on whether the surnames of the individuals are recorded or whether the voice could lead to identification of the individual.

SPECIAL CATEGORY (sensitive) PERSONAL DATA

Refers to race/ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and offences (alleged or committed). The definition of health data includes genetic and biometric data.

DATA PROTECTION PRINCIPLES

Everyone responsible for using personal data has to follow the 'data protection principles'.

They must make sure the personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR/DPA 2018 in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

PROCESSING PERSONAL DATA

Means obtaining, recording or holding data or carrying out any operation or set of operations on the data including the organisation, adaption or alteration of the data; retrieval, consultation or use of the data; disclosure of the data by transmission, dissemination or otherwise making available; alignment, blocking, erasure or destruction of the data.

It is difficult to think what an organisation might do with the data that would not be defined as processing.

If you process data, you will be a data controller or a data processor.

DATA CONTROLLER

A person who alone, jointly or in common with others, determines the purposes for which and the manner in which any personal data is processed. Data controllers will usually be organisations, but can be individuals. The data controller must also be responsible for and able to demonstrate compliance with the principles above. Two organisations acting together to decide the purpose and manner of any data processing would be joint data controllers.

DATA PROCESSOR

Any person (other than an employee) who processes data on behalf of the data controller.

Depending on its role an agency may be a data controller or a data processor when working with a commissioning client company.

CONDITIONS FOR DATA PROCESSING

Those processing personal data must have a 'lawful basis' for doing so and this must be documented, these include:

- Consent of the data subject
- Processing is necessary for the purposes of the legitimate interests of the data controller or a third party

Other bases such as - processing is necessary for the performance of a contract, for compliance with a legal obligation, in relation to legal proceedings, to protect the individual's vital interests, for the performance of a task carried out in the public interest (these conditions are unlikely to apply to MR or data analytics).

If the information is special category (sensitive) personal data, at least one of several other conditions must also be met before the processing is considered fair and lawful. Of these additional conditions the two most likely to apply to market research or data analytics is that the individual whom the sensitive personal data is about has given explicit consent to the processing or there are legitimate interests.

CONSENT I.E. INFORMED CONSENT

Consent under GDPR/DPA 2018 refers to "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

PRIVACY NOTICE

The statement – oral or written - that individuals are given when data about them is collected. When using and sharing personal data the privacy notice must tell the individual - who you are, the purpose(s) for which you intend to process the information; and any extra information you need to give individuals in the circumstances to enable you to process the information fairly.

SHARING CUSTOMER DATA

Disclosure of personal data from an organisation to a third party organisation(s) or the sharing of personal data within an organisation.

ANONYMISATION

Removing, obscuring, aggregating or altering identifiers. Once all identifiers linking data to an individual have been removed then it is no longer personal data - it has been anonymised) and is not covered by data protection law.

The Market Research Society have cautioned members that they *must take reasonable steps to ensure that anonymisation is effective, with reference to developments in technology and to the data environment into which data are released.*

PSEUDONOMISATION

Personal data is removed and the 'record' is given a unique identifier. If personal data has been pseudonymised it will still be considered personal data if you retain the ability to re-identify the individual.

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/

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 onlv.

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