BHBIA Ethics & Compliance

Preparing for the General Data Protection Regulation

BHBIA Checklist to help you audit your data processing

Introduction

The General Data Protection Regulation (GDPR) will apply from 25 May 2018. Both data controllers and processors will be required to demonstrate that they process personal data in compliance with the GDPR.

The first step in preparing for the GDPR is to make sure that you understand what personal data you process. The BHBIA's Ethics & Compliance Committee recommends that you audit - review and take stock of - the personal data you handle.

This is an important step, it will help you to identify what you have to do to prepare for introduction of the GDPR. And it's important to be prepared . . .

> *"There's a lot in the GDPR you'll recognise from the current law, but make no mistake, this one's a game changer for everyone."*
>
> Elizabeth Denham, UK Information Commissioner, 17 January 2017

The BHBIA will only address the impact of the GDPR on market research and data analytics. Other areas impacted by the GDPR e.g. employee data, are considered out of scope for the BHBIA.

Checklist to help you audit your data processing

To help you audit your personal data processing, we've compiled a list of questions – see overleaf.

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 ensure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA. We do expect to update our guidance on the GDPR as more information becomes available.

BHBIA Ethics & Compliance

Checklist to help you audit your data processing	
What you need to know	***Why you need to know this under GDPR***
'PD' refers to personal data	
Your role	
Are you/is your organisation acting as a sole or joint data controller or a data processor?	*As a controller or processor you should understand your responsibilities and liabilities, they may differ in some respects* *Extensive terms need to be included in contracts between controllers and processors*
If you're not a data controller, who is and do you have their contact details?	*This information must be supplied to secure the informed consent of the data subject*
If you're a data processor, do you subcontract to other processors?	*Processors must have the written consent of the controller to appoint sub-processors* *Sub-processors e.g. freelancers will be required to adhere to the GDPR too*
Source and types of data	
What is the source of the PD you hold (e.g. data subject, client, publicly accessible source, social media platform/space)?	*The information that must be provided to secure informed consent and the time at which it must be given, can vary depending on where the PD is obtained from*
What types of individuals (e.g. adults, children) do you hold PD about?	*There are different requirements for different types of individuals*
What types of PD (special categories/sensitive data such as health records) do you hold?	*Contracts must document the specifics of the data processing*
Type and purpose of processing	
What types of processing do you undertake e.g. collecting, recording, storing, analysing?	*You will have to keep detailed internal records of processing activities*
What is the purpose of the data processing?	*This will limit what the data can be used for*
Do you make any decisions based on automated processing or profiling of individuals?	*Privacy Impact Assessments will be mandatory for automated processing that result in automated decisions that have a significant impact or legal effects*
High risk data processing	
Do you carry out 'high risk' data processing - this might involve sensitive data, vulnerable individuals or children, processing PD on a large scale or automated profiling of individuals?	*You may need to appoint a Data Protection Officer* *You will need to complete privacy impact assessments for riskier activities* *You will need to be able to identify the value and sensitivity of the data as well as threats to it*
If their PD was disclosed how likely is it and how severe would any harm be to data subjects (e.g. reputational damage, loss of confidentiality)?	

Your legal basis for processing	
What is the basis you use for data processing – consent, legitimate interests or research exemption?	*You must have a legal basis for processing PD* *The legal basis will affect what you can and can't do with the data*
Is consent 'verifiable' – do you have a record of how and when consent was given?	*You will be required to have verifiable consent and keep records of it*
What rights has the data subject been told they have?	*Data subjects must be clearly informed of all their rights – access, rectify, erasure, restrict processing, data portability, to object*
Data minimisation	
Do you pseudonymise the PD as soon as possible?	*You will need to pseudonymise PD as soon as possible (but remember pseudonymised data is still PD if you have the means to reverse the pseudonymisation)*
Have you collected any non-essential PD?	*Data minimisation will be required*
Record keeping	
Do you keep a record of the PD you process?	*You will need a detailed and documented record keeping process because demonstrable processes to ensure accountability will be required*
Sharing PD and transferring it overseas	
Who is the PD shared with?	*PD received must be limited as far as possible*
Do you transfer PD to other countries, if so which ones and are they outside the EEA?	*Onward transfer of PD must be limited* *You must adhere to cross border requirements and restrictions*
Do you have a policy/process in place if you receive a request for access to or erasure of PD?	*Systems must be able to cope with the new rights to data portability, the right to be forgotten and they must record objections or withdrawal*
Access, storage and security	
Where is the PD stored?	*Appropriate safeguards – technical and organisational – will need to be in place* *All PD must be kept secure* *Physical (e.g. locked doors) and virtual security (e.g. encryption) is required* *Virus and perimeter protection (e.g. firewalls) should be used*
Who has access to it?	
How is access controlled?	
How is it kept secure (what technical and organisational methods do you use)?	
Is the PD accurate and up to date?	*You must maintain accurate and up to data databases*
How long will the PD be retained for?	*Contracts must document duration of storage* *You must have clear data retention policies* *Storage should be limited*
Do you have a data retention policy?	
How do you make sure PD is securely deleted or returned?	*You must have clear data deletion policies*
Data breaches	
What would you do if PD was lost or disclosed accidently?	*You will be required to have a data breach detection, investigation, internal reporting and notification process in place* *Certain types of data breach must be reported to the ICO and sometimes to the data subject*

Checklist to help assess security

Published within the MRS/SRA Data Protection Act 1998: Guidelines for social research, October 2005

Researchers should consider the following checklist regarding security when assessing whether their technical and organisation measures are appropriate:

⇒ Are the automated systems protected by a level of security appropriate to the data held?

⇒ Are technical measures in place to restrict access to systems holding personal data?

⇒ Are technical measures in place to secure data during transit (e.g. to subcontractors and interviewers)?

⇒ How is the data stored by your sub-contractors and interviewers – is it adequate and appropriate?

⇒ Are the premises on which the data is held secure?

⇒ Is access to the premises restricted?

⇒ If the data is held on non-automated systems e.g. paper files, discs, microfilm, and microfiche, is access still restricted or secure?

⇒ Are copies of printouts, obsolete back-up tapes etc. disposed securely?

⇒ Is obsolete hardware and software from which data could be recovered disposed of securely?

⇒ Is there an auditable data retention and destruction policy?

⇒ Are staff trained and made aware of their responsibilities to safeguard the personal data?

Sources and references for further reading

- Five questions to ask when starting a GDPR Compliance Project, MRS
- Adopting a Risk-Based Approach to GDPR, MRS
- GDPR Compliance Timeline, MRS

Prepared by the BHBIA's Ethics & Compliance Committee May 2017

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