BHBIA Personal Members GDPR WebEx

17 November 2017

Q&A

BHBIA Ethics & Compliance

Definitions

1. What data are considered to be personal and sensitive?

The GDPR definition of 'personal data' is:

> The GDPR defines personal data as '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*; (Article 4)
>
> *'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.* (Article 4)
>
> *'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.* (Article 4)
>
> *'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.* (Article 4)
>
> Special categories of personal data (previously sensitive personal data) - *data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.* (Article 9)
>
> *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not*

apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes. (Recital 26)

Special category (previously referred to as sensitive) personal data includes racial or ethnic origin, political opinion, religious beliefs, membership of a trade union, physical or mental health or condition, sexual life. Personal health data includes all data pertaining to health status which reveals information relating to past, current or future physical or mental health status e.g. disease, disability, disease risk, medical history, clinical treatment. It also includes genetic and biometric data.

Key points for personal members to take on board are that:

- Personal data may be made up of more than one piece of information e.g. a job title and a place of work together could identify an individual.
- Pseudonymised data will still qualify as personal data if you have the ability to reverse the pseudonymisation (i.e. you/your organization has the information that would re-identify individuals)

2. What are the roles of Data Controllers and Data Processors?

Data Controllers determine the purpose and means of data processing, so for example, if you influence the design of the work or you maintain a list of potential respondents you are a data controller.

Data controllers are:

- Responsible for and able to demonstrate compliance with GDPR
- Point of contact for data subjects
- Determine if and conducts Privacy Impact Assessment required
- Can audit processor

Data Processors process the data on behalf of the data controller, so if you only act on the instruction of others (such as a market research or fieldwork agency), you are a data processor.

Data processors must:

- Seek approval to appoint sub-processor
- Include GDPR obligations in sub-processor's contract
- Seek approval to transfer personal data out of EU

Both Controllers and Processors must:

- Implement technical and organisational measures
- Make sure contracts contain the right detail
- Appoint Data Protection Officer if this is required
- Keep detailed records
- Build in privacy by design and default
- Have a legitimate basis for data processing

– Maintain and store data and records

If a company commissions market research from an independent agency and this agency then conducts all the work on their behalf (under contract) and supplies the company with only aggregated anonymised data (i.e. the company does not have access at any stage to any of the personal data collected by the MR agency), the client company is a data controller as is the agency.

Although the data which the commissioning company will see is anonymised and aggregated, the collection, storage and other processing of personal data is happening for the commissioning company's overall purpose – without this purpose the processing would not be undertaken at all. The MR agency is applying technical expertise to the selection, processing and interpretation of personal data meaning they would also be data controllers (e.g. making a number of decisions about who, what, where, when and how personal data is processed as part of the project including the application of MR methodologies and design of any questions/interviews).

3. Who is the ICO?

The ICO is the Information Commissioner's Office. The ICO is the UK data protection supervisory authority or regulator. The ICO is an independent body set up to uphold information rights in the UK. It is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport.

4. How long can personal data be stored?

Personal data should not be kept longer than necessary irrespective of where or how it is stored. Different companies may have different data retention requirements. There are no absolute guidelines on lengths of time quoted within the GDPR or from any regulator, nor do we expect to receive any. The period of time should be agreed between the data controller and data processor. This is not a new requirement and should apply to all stored personal data (i.e. that stored per and post GDPR).

Secondary Data

5. What are the implications of the GDPR for the processing of secondary data that includes personal data?

Broadly speaking GDPR requirements are the same for the processing of secondary data for data analytics as for primary data for market research. The BHBIA recommends that those involved in data analytics processing secondary data:

- Audit systems and work out where you are processing personal data
- Risk assess your processes and if necessary complete privacy impact assessments
- Review contracts with third party controllers / processors and ensure there is adequate clarity regarding roles and expectations

For further detail and specific secondary data examples please see the 'Implications of GDPR For Data Analytics' presentation prepared and delivered by Matt Beckett on the 7 September at the BHBIA GDPR Seminar Building the GDPR into every stage of your project and available to

members on the BHBIA website
https://www.bhbia.org.uk/archive/eventarchive/gdprseminar2017.aspx

Notification & Contracts

6. Do you need to register yourself as a data controller and/or processor with the ICO if you are a freelancer?

The current notification requirements are as follows:

Most organisations that process personal data must notify the ICO of certain details about that processing. However, the Act provides exemptions from notification for:

- *organisations that process personal data only for:*
- *staff administration (including payroll);*
- *advertising, marketing and public relations (in connection with their own business activity); and*
- *accounts and records;*
- *some not-for-profit organisations;*
- *organisations that process personal data only for maintaining a public register;*
- *organisations that do not process personal information on computer.*

Exemptions are also available in relation to:

- *national security and the armed forces;*
- *personal data that is processed only for research, statistical or historical purposes;*

https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/

Under GDPR, this is what we know at present about new notification requirements:

When the new data protection legislation/GDPR comes into effect next year there will no longer be a requirement to notify the ICO in the same way. However, a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee.

The current draft proposal is a three tier system, which will differentiate between small and big organisations and also how much personal data an organisation is processing. The aim is to keep the system as simple as possible, so that organisations will easily be able to categorise themselves.

https://iconewsblog.org.uk/2017/10/05/ico-fee-and-registration-changes-next-year/

The ICO expects to know more by the end of 2018 and will communicate further when they do.

7. What terms/changes might we need to make to our contracts?

Expect contracts under GDPR to include:

– Details of specific processing - subject matter, duration, nature, purpose, type of data & type of data subjects

- Risk & DPIAs requirements
- Information necessary to demonstrate compliance
- Safeguards - technical & organizational incl. confidentiality
- Retention, return, deletion requirements
- Data breach notification
- Inspection & auditing requirements
- Liabilities, assurances & indemnities for legal action
- Respective responsibilities of joint controllers

Data processors need the data controller's written consent to appoint sub-processors e.g. freelancers – they must adhere to GDPR too, and processor's must have contracts with named sub-processors too.

GDPR is not clear about whether the obligation to include processor clauses in contracts falls on the controller, the processor or both. The GDPR simply says these clauses must be included - so it is possible that both the controller and the processor must ensure they are included.

Risk Assessment

8. Is a Data Protection Impact Assessment (DPIA) required for data processing authorized before May 2018?

Current data protection guidance advocates a risk-based approach including risk assessment but conducting a PIA is not a legal requirement of the Data Protection Act. The GDPR formalises the need for DPIAs and makes it a requirement in some cases. See further information below.

If after 25 May 2018 you continue to rely on risk assessments and DPIAs carried out before this date, you must make sure that these are GDPR compliant. If they are not, you must update your risk assessments and DPIAs. We advise you to update your risk assessment processes and tools that you will rely on after 25 May 2018 as soon as practical if they aren't GDPR compliant.

Taken from the BHBIA's 'Risk and Privacy Impact Assessment' guidelines, within the Preparing for the General Data Protection Regulation series, available on the BHBIA website.

DPIAs MUST be carried out when:

- Large scale processing of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to their rights and freedoms
- Large scale processing of special categories of data (previously referred to as sensitive data)
- Using new technologies and the processing is likely to result in a high risk to rights and freedoms
- Automated processing, including profiling, that results in automated decisions having legal effects or similar significant impacts on the data subjects
- The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual (e.g. personalised targeted direct mailings), profiling is not the same as market research segmentation.
- Systematic monitoring of a publicly accessible area on a large scale.

Respondents' Rights

9. What is the difference between asking not to be contacted and asking for your personal data to be erased?

Under GDPR individuals have a new right to erasure, also known as the right to be forgotten. This gives the individual the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals also have a right to restrict processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

If an individual asks not to be contacted for the purpose of market research they are exercising their right to restrict processing (not their right to erasure). It is important not to confuse the two different rights. Quite clearly if you are going to observe a request not to be contacted for the purposes of market research you will need to store some personal data to do this.

Preparing for GDPR

10. How will GDPR will affect personal members/freelancers and what should we be doing to prepare?

Broadly speaking the GDPR will affect individuals processing personal data in largely the same way that it impacts organisations. There may be some differences in terms of record keeping (see the notes below) and risk assessment requirements (if large scale processing of personal data is not undertaken) but on the whole the requirements do not vary with the size of the organisation.

The BHBIA advises personal members to:

a. Understand your role and audit the data processing you do
b. Put the necessary processes in place
c. Document what you do however if your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing although contractual requirements may require all suppliers in the chain to keep detailed records – do check!

The first step is to understand or review your current position in order to know what it is you need to change in order to be GDPR ready.

- Review or audit what data processing you do:
  - Your role
  - Source and types of data
  - Type and purpose of processing
  - High risk data processing
  - Your legal basis for processing
  - Record keeping

- Sharing personal data and transferring it overseas
- Access, storage and security

Once you've done this you're in a position to assess the risk associated with your data processing which will mean carrying put Privacy Impact Assessments for higher risk activities, and then you're in a position to think about what you will have to do to mitigate these risks

You may have identified some gaps in your policies and procedures that need to be filled e.g. your security systems and record keeping may not be up to GDPR standards.

You should now be in a position to develop a GDPR action plan detailing the changes you need to make to be GDPR ready. You may need to prioritise what you do according to risk.

The changes you may have to put into place could include:

- Amending contracts / MSA templates
- Updating policies and processes e.g. data retention, data breach
- Updating consent statements and privacy notices
- Building privacy by design and default into all new projects

The ICO has made available a series resources to help small organisations get to grips with the GDPR, these include:

- getting ready for the GDPR self help checklist
- '12 steps to take now'
- advice service helpline for small organisations

In addition, the ICO has a series of data protection guidance resources available for small businesses (these relate to the Data Protection Act rather than the GDPR but still provide very useful information):

- Getting it right: a brief guide to data protection for small businesses
- Getting it right: small business checklist
- Personal information online: small business checklist
- A practical guide to IT security: ideal for the small business
- Training checklist for small and medium-sized organisations

This document is provided for information purposes only. The responses do not include any regulatory or legal advice and should not be construed as such.

Prepared by Catherine Ayland on behalf of the BHBIA, 11 December 2017