BHBIA Ethics & Compliance

Data Protection Requirements

Data Security, Breaches and International Transfers
February 2022

Introduction

The UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act (DPA) 2018 require that personal data is collected, used, transferred, stored and destroyed securely by using "*appropriate technical and organisational measures*" to protect it from unauthorised or unlawful processing, accidental loss, misuse, destruction and damage. Personal data must be kept secure throughout its processing life.

These guidelines detail UK GDPR/DPA 2018 requirements for data:

- ***Security***
- ***Breaches***
- ***International transfers***

However we would like to stress that one of the best ways to minimise security risks is to minimise the collection, storage and transfer of personal data and process only that which is essential.

Data security

The security measures you put in place should take into account the:

- Threats to, value and sensitivity of the data
- Damage that could be caused to individuals if there is a security breach
- State of the art, the costs of implementation and the nature, scope, context and purposes of the data processing.

Consequently there is no one set of security measures that will suit all situations.

Key considerations for data security

When reviewing your data security requirements you should consider:

- Physical security for the premises/office, desk, personal computers, mobile devices e.g. clean desk and locked doors and drawers policies
- Virtual security for computers and mobile devices e.g. strong individual passwords (linked to types/levels of access) including password storage and changing rules; and encryption (which protects data stored on mobile and static devices and in transmission), screen locking when absent from the desk
- Use of individual's own device guidance
- Perimeter protection e.g. firewalls and gateways
- Anti-virus and anti-malware protection
- Software updates and patch management
- Where and how data is stored e.g. filing systems and structures, including cloud storage
- Off-site back-up (European Union (EU) based)
- Logging of access and processing activities by individuals
- Secure data transfer and file sharing arrangements e.g. file transfer protocols (FTPs) or Virtual Private Networks (VPNs), although it is important to remember that without additional encryption in place the data will only be encrypted whilst in transit
- Siting of fax machines in safe/secure areas
- Secure means of disposal/destruction of redundant equipment (e.g. DPUs, USBs) and data
- Disaster recovery i.e. "*the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*"
- Companies may want to work to a prescribed data security framework/quality standard e.g. ISO27001
- Who data is shared with
- Commitments from those sharing data to protect it appropriately and use it only for the lawful and intended purposes e.g. confidentiality agreements, observer agreements

Oversight and training

There are a series of practical steps you can take to make sure that the most appropriate security measures are used:

- **Carry out a security audit** of the systems containing your data. This will help to identify vulnerabilities which need to be addressed.
- **Security policy and processes** should be documented.
- **All staff, new and existing, should be trained** (including sub-processors) and made aware of their responsibilities to safeguard personal data using the measures and systems available.
- **Carry out internal security audits** to monitor compliance; organisations should have in place "*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*."

Further information

Whilst not UK GDPR/DPA 2018 specific the following Information Commissioner's Office (ICO) guidance is currently being recommended until updated UK GDPR-specific guidance becomes available: **https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf**

On encryption specifically **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/**

Breaches

The UK GDPR/DPA 2018 makes it clear that those processing personal data must have appropriate measures in place to keep the data secure. The ability to detect, address and report a breach in a timely manner is an important part of these measures.

Definitions

A "personal data breach" is "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". Breaches may be accidental or deliberate.

- Destruction means the data no longer exists or no longer exists in a form that is of any use to the controller/processor
- Damage refers to the data being altered, corrupted or is no longer complete
- Loss" means the data may still exist, but control of it or access to it has been lost or it's no longer in the possession of those that should have it
- Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the UK GDPR/DPA 2018.

A data breach can result in emotional distress, physical or material damage to the data subject, including loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality and economic or social disadvantage.

Breach protection process

Those processing personal data should put in place a process to:

- Detect a breach
- Quickly contain the breach and recover the situation
- Assess the risk to data subjects
- Decide whether to notify the competent supervisory authority and inform data subjects
- Document data breaches, including:
  - the causes
  - what happened
  - personal data affected, including the types and numbers of records and individuals
  - the consequences and potential consequences of the breach
  - remedial action taken – to deal with breach and mitigate its impact
  - explanation of the decision to notify or not to notify
- Provide this documentation to the authorities if they are to be notified. It is recognised that it may not be possible to investigate a breach fully within 72 hours, so supplying the information required can be done in phases but must be done as soon as possible.

- If data subjects need to be informed of the breach, they should be given the name and details of a contact person (usually the Data Protection Officer), details of the likely consequences of the breach and the measures taken to deal with it, and its impact.

There should also be a person or team responsible managing data breaches.

Data Controllers and Data Processors Roles

The European Data Protection Board (EDPB) have advised that:

- Becoming 'aware' of a breach begins when the Data Controller has a reasonable degree of certainty that the security of the personal data has been compromised.
- If a Data Processor is used by the Data Controller and the Processor becomes aware of a breach (of the personal data it is processing on behalf of the Controller), it must notify the Controller "*without undue delay*".
- As the Controller uses the Processor to achieve its purposes, the Controller should be considered aware once the Processor has become aware.
- A Processor could make a notification on behalf of the Controller but only if this has been authorised by the Controller and it is part of the contract. Legal responsibility to notify remains with the Data Controller.

Timeframe for notification

If a data breach is likely to result in damage to the data subject the Data Controller must notify their lead supervisory authority of the breach within 72 hours of becoming aware of it. Given that there may be several parties involved in the market research chain, meeting the 72 hour requirement could be difficult and it may be advisable to have a contract clause that commits all parties to timely reporting.

If there is a high risk that damage to individual is likely, the Data Controller must communicate the breach to the affected individuals as soon as possible.

Further information

For further information see the EDPB *Guidelines on Personal data breach notification under Regulation 2016/679* Adopted on 3 October 2017, **https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052**

For more general information on breach reporting see the Information Commissioner's Office (ICO) UK GDPR guidance at **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/?q=breach**

International data transfers

Many organisations involved in market research and business intelligence need to transfer personal data from one country to another. Although it is always worth asking whether this is essential!

The UK GDPR/DPA 2018 imposes restrictions on some transfers of personal data overseas to make sure that protection travels with the data.

The following guidance details how to make sure that personal data is kept secure and processed in line with UK GDPR/DPA 2018 requirements when you transfer it outside the EU.

Data transfers from the EU to the UK

The UK's data protection regime has now been formally deemed 'adequate' by the EU.

An adequacy decision allows organisations that transfer personal data from the EU (and the European Economic Area EEA) to the UK, to continue to do so; there is no need to put alternative transfer mechanisms (such as standard contractual clauses (SCCs)) to be put in place.

Data transfers from UK to EU

These transfers have continued irrespective of the adequacy decision without the need for any additional safeguards because the UK has already designated EEA member countries as providing an adequate level of protection (of personal data for the purposes of the UK GDPR).

In addition, the UK has adopted the same adequacy decisions as the EU and so transfers can be made from the UK to these 'adequate' countries e.g. Japan, without additional safeguards.

Data transfers from the UK to third countries

For transfers of personal data to those countries not covered by an adequacy decision (known as 'third countries'), an alternative means of keeping the data secure to UK standards needs to be put in place.

In July 2020 the 'Privacy Shield' was judged invalid by the EU Court of Justice (EUCJ) and so can no longer be used to safeguard transfers of personal data between EU and US organisations. The USA is a third country.

The most likely alternative means are EU Standard Contractual Clauses (SCCs) or EU Binding Corporate Rules (BCRs).

EU Standard Contractual Clauses

SCCs can be used as they are recognised in UK law and are likely to be the most appropriate alternative. These approved clauses enable the free flow of data when included in a contract or added as an appendix to a contract. They cover the contractual obligations between both parties to protect the rights of the individuals whose data is being transferred.

Updated EU SCCs have been developed by the European Data Protection Board (EDPB) and are now available. For more information on these see https://www.bhbia.org.uk/resources/news/data-protection-news-new-eu-standard-contractual-clauses-sccs

However, the new EU SCCs will not apply for transfers of personal data *from the UK* to a third country. The ICO has published new UK specific data transfer mechanisms which come into force on 21 March 2022. For further detail please see the '*International data transfer mechanisms under the UK GDPR*' guide available on the BHBIA's website on the Privacy and Data protection webpage.

Supplementary measures for SCCs

In July 2020 the EUCJ ruled that the use of SCCs needs to be assessed on a case-by-case basis and that "supplementary measures" e.g. encryption, might be necessary to protect the data subject.

Basically it is important to make sure that SCCs are fit for purpose and that they do genuinely provide the security intended. So, a data exporter should consider whether and what additional security measures are needed when transferring data to a third country. Determining those measures will largely depend on the data protection regime in the receiving country.

EU Binding Corporate Rules

Binding Corporate Rules (BCRs) may also be an option for some organisations or group of enterprises engaged in a joint economic activity. BCRs authorised before 31 January 2020 can be used as they too are recognised in UK law.

Other options

Other options such as a GDPR Code of Conduct, the use of a derogation or the research exemption are either unavailable or likely to be of limited value in healthcare business intelligence at present. The UK's Market Research Society (MRS) is working on the development of a GDPR Code for social, opinion and market research which may for those that sign up to it provide a means to secure unrestricted data transfers.

Advice to BHBIA members

- Identify cross border data transfers your organisation makes/is likely to make.
- Review contracts with partners based overseas to check that they include transfers of data to the UK (an ex-EU/EEA country granted EU adequacy status).
- Update your data protection agreements to make sure that they allow for the transfer of personal data to the UK and include the correct details for Data Protection Officers, local representatives and/or lead supervisory authorities.
- Revise privacy notices so that data subjects are informed of the transfer of their personal data outside the EU.
- Privacy notices, internal policies, contracts and other documents may need to be updated to reflect the applicable regime(s).
- Organisations relying on BCRs for transfers to territories outside the EU/UK may need to have those rules validated by the ICO or an EU supervisory authority.

Further information

ICO's International data transfer agreement and guidance available: **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/**

Subject to change

The BHBIA's guidance is subject to change. We will do our best to keep members up to date but please monitor news from the ICO https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/statement-on-data-protection-and-brexit-implementation-what-you-need-to-do/

Updated by the BHBIA's Ethics & Compliance Committee February 2022

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