BHBIA Ethics & Compliance

Preparing for the General Data Protection Regulation

GDPR – Data Security including Breaches and International Transfers

Introduction

The GDPR requires 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 GDPR 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, PC, 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 (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 GDPR specific the following ICO guidance is currently being recommended until updated 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/encryption/**

Breaches

The GDPR 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 GDPR.

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.

Roles' of Data Controllers and Data Processors

The Article 29 Data Protection Working Party 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 Article 29 Data Protection Working Party *Guidelines on Personal data breach notification under Regulation 2016/679* Adopted on 3 October 2017, **http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083**

For more general information on breach reporting see the ICO's 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 GDPR imposes restrictions on the transfer of personal data outside the European Union (EU) 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 GDPR requirements when you transfer it outside the EU.

Transfers and restrictions

International transfers of personal data for processing may be made to:

1. Countries within the EU with no restrictions
2. Non-EU countries where the European Commission (EC) decides that an adequate level of data protection is provided, this 'adequacy decision' establishes that a non-EU country provides a level of data protection that is essentially equivalent to that in the EU
3. Organisations in countries not covered by 1 and 2 above where appropriate safeguards have been put in place e.g. EU model clauses
4. Organisations in countries not covered by 1 and 2 above where exceptions can be made because specific conditions apply e.g. the transfer can be made as the data subject has given their informed consent

Transfers on the basis of a European Commission adequacy decision

International transfers of personal data may be made where the EC has decided that a third country (a non-EU country), a territory or one or more specific sectors in the third country, or an international organisation ensures an 'adequate' level of protection.

All countries belonging to the European Economic Area – the EEA (which includes the 28 EU member states plus Iceland, Liechtenstein and Norway) – are considered by the EC to have adequate data protection in place so there are no restrictions on transfers to and processing of the personal data of EU citizens within these countries. Similarly, the following non-EEA countries are also considered to have adequate data protection in place – Andorra, Argentina. Canada, Faroe Islands Guernsey, Isle of Man, Israel, Jersey, Switzerland and Uruguay.

Authorisations of transfers made by EU member states or supervisory authorities and decisions made by the EC regarding adequate safeguards made under the Data Protection Directive will remain valid/remain in force until amended, replaced or repealed. So until the EC tell us otherwise (http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358), adequacy decisions in place currently will remain in force when the GDPR takes effect (after 25 May 2018).

Transfers subject to appropriate safeguards

You may transfer personal data when the organisation receiving it is subject to appropriate safeguards and on condition that enforceable data subjects' rights and effective legal remedies are available. The appropriate safeguards include:

- Standard contractual clauses (SCCs), data protection clauses adopted by the EC or a supervisory authority and approved by the EC
- Binding corporate rules (BCRs), agreements governing transfers made between organisations within the same corporate group or a group of enterprises engaged in a joint economic activity but not necessarily forming part of the same corporate group

Under GDPR there is no longer a requirement to give prior notification to and seek authorisation from Data Protection Authorities when transferring personal data to a third country based on SCCs or BCRs.

The GDPR also introduces new safeguards for international transfers for use under certain conditions but these are less likely to be immediately relevant to healthcare market research. They include compliance with an approved code of conduct or certification mechanism to establish appropriate safeguards. There are additional provisions for public authorities but again, these too are unlikely to be relevant to commercial market research.

Other transfer options – derogations

The GDPR provides derogations – exemptions – from the general prohibition on transfers of personal data outside the EU for certain specific situations:

- Made with the individual's informed consent after having been informed of the possible risks associated with such a transfer in the absence of an adequacy decision and appropriate safeguards
- Necessary for the performance of a contract:
  - between the individual and the organisation
  - made in the interests of the individual between the controller and another person;
- Necessary for important reasons of public interest
- The transfer is made from a register available to the public or any person with a legitimate interest
- Necessary for compelling legitimate interests of the Data Controller - in certain very specific circumstances - if no other transfer means is available and the transfer is one-off or infrequent and involves only the data of a limited number of individuals.

There are other derogations but these are unlikely to be relevant to commercial healthcare market research.

Consent agreements and privacy policies must include details of any transfer outside the EU, the country should be named and if possible in the privacy policy a link to the adequacy mechanism used should be provided. In addition, details of safeguards (or at least a link to them) should also be provided.

Transferring personal data to the USA

The USA does not have an EC Adequacy decision due to differences in US privacy laws. In the USA the 'Privacy Shield' (which replaced the Safe Harbor agreement) can be used for transfers between EU and US organisations. This mechanism is only available when processing data in the USA, and only where the receiving US organisation has been through the process of self-certifying themselves with the US Department of Commerce. By doing so they are committing themselves to the standards of data protection required by the EU, which is enforceable under US law.

Practical steps to take

Organisations should:

- **Review and map international transfers** of personal data
    - bear in mind that data processing includes storage of data and backups, so overseas servers or cloud systems should be taken into account.
- **Review current transfer mechanisms** to make sure they are GDPR compliant
- **Amend and update privacy notices** (consent agreements and privacy policies) to include details of transfers to third countries and safeguards.

Further information

See the European Commission's data protection website at: **http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm**

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Exchanging and Protecting Personal Data in a Globalised World, 10.1.2017 **http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN**

For UK information from the ICO on international data transfers **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/?q=transfer**

For information on EC approved SCCs see **https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en**

For information on EC BCRs see Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, wp256

For more details about the Privacy Shield **https://www.privacyshield.gov/Program-Overview**

Prepared by the BHBIA's Ethics & Compliance Committee April 2018

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