BHBIA Guidelines for the Use of Secondary Data
Processing Personal Data Outside of the UK

These guidelines are part of a series designed to provide clear guidance on the legal and ethical implications of using secondary data for market research and associated business intelligence purposes such as database building or customer relationship management.

Many organisations involved in business intelligence need to transfer personal data from one country to another. Although it is always worth asking:

- Whether the purpose be achieved without the use of personal data?
- Can the data be anonymised so that data protection requirements don't apply?

The GDPR imposes restrictions on the transfer of personal data outside the European Union (EU) to make sure that protection travels with the data.

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

Processing includes storage of data and backups, so servers or cloud systems used to store personal data need to reside in approved countries too in order to avoid the need for additional arrangements.

If you are processing data in a non EU country or a country without an adequacy decision, you will need to consider the following:

- Data subjects will need to be informed that their data is being processed in the relevant country
- Security arrangements for the transfer of data will need to be considered and documented (e.g. use of encryption technology). Privacy notices must include information about details of any transfer to a third country plus details of the safeguards and the means by which to obtain a copy of them or where they have been made available.
- An appropriate contractual arrangement needs to be in place with the company receiving the data (see below)

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 will remain in force 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.

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 business intelligence.

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.

Examples

1. A UK based data collection and processing company has decided to out-source their UK personal data processing to a third party based in India (for marketing segmentation & targeting activities).

   Prior to sending any personal data from the UK to India the UK company should determine if this activity cannot be achieved by using anonymised data. If not then the UK company must establish a contract with the Indian company that ensures adequate protection under the UK Data Protection Act. This may involve self-assessment; contractual clauses and Binding Corporate Rules approved by the Information Commissioner's Office or be covered by exceptions from the rules.

2. A global CRM company has sold its on-line software and applications platform to a UK pharmaceutical company. The CRM servers will be based in Belgium and personal data from the current UK based system will be transferred to the Belgium platform.

   Belgium is a member state of the European Union and as such personal data can be transferred from the UK to Belgium without restrictions.

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

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,

Matt Beckett, Data Analytics Team Lead
Darren Kottler, Data Analytics Team
Jason Bryant, 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 Guidelines > Request Advice. Please note: this ad hoc advisory service is available to full BHBIA members only.

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