Title:	Data Policy, Quick Guide
Partner Responsible:	Data Governance Working Group
SP / WP / Task Involved:	all SPs

Authors:	Jan Bjaalie, Kevin McGillivray, Bernd Stahl, Tyr Fothergill
Contributors:	SP12 EAB
Editor:	B. Stahl, T. Fothergill

Document Approval Status

Date	Comments
14.03.2018	First draft of document
	Submitted to the EC for Review

1. Introduction

The HBP is a multifaceted research project, involving several categories of data in a complex ICT environment. Although legal and ethical requirements vary depending on the type of data collected, the HBP focus on compliance does not. A core thread running through the HBP is compliance with all applicable national, European, and international regulations concerning data, depending upon the data type, e.g. whether that data is human or animal. The following Data Policy Quick Guide provides an overview of the core requirements HBP partners have regarding the data supplied or consumed in the project. Following extensive work on the principles and practices of data policy in the Human Brain Project (HBP) which led to the ongoing development of the Data Policy Manual, a decision was taken to extract the relevant policies and combine them in this document. The purpose of the document is to give a clear and concise description of the relevant policies for use by HBP scientists. This document keeps references and background information to a minimum. It is based on the Data Policy Manual, which remains valid and contains the background information, definitions, references etc. which are not present in this document. For more detailed information, please check the Data Policy Manual.

The policies described in this document were developed with particular attention to the work of the neuroinformatics platform (NIP, SP5), but they apply to all data in the HBP. Outside of

SP5 they may need to be adapted appropriately, which is the responsibility of the SPs and PIs.

The policies focus on two main items:

- Model organism data (animal data)
- Data protection (human data)

The HBP adopts the policies set out in this document in order to:

- Facilitate the formal publication of data sets, as well as enabling the tracking of their usage through citation, data licenses, and ethical approvals.
- Support transparency and openness of the research it undertakes.
- Ensure continuing availability of data (with the intent of securing sustainable long-term use, teaching, further research, public access, reproducibility, etc.).
- Ensure that expectations with regard to data handling are transparent and accessible.
- Comply with all data-related regulations and legislation, in particular those related to data protection.
- Ensure that all data registered and used in the HBP comply with ethical and legal requirements.

Furthermore, this document aims to reconcile ethical and legal requirements with the FAIR Guiding Principles for scientific data management and stewardship[1] and implementation-level policies described in the Research Data Alliance (RDA) Practical Policy[2] document.

Data policy for large and international collaborations in neuro-ICT involving technical, animal and human data raises many questions that are not fully settled. The HBP data policies will therefore need to be continually monitored and developed; these changes will be reflected in this document.

[1] https://www.nature.com/articles/sdata201618

[2] https://www.rd-alliance.org/group/practical-policy-wg/outcomes/practical-policy

2. Model Organism Data

2.1. Data Contributors

Data Contributors in the HBP are the PIs of the project, or the persons whom they appoint to represent them. It is assumed that task leaders are PIs unless other information is provided.

The responsibility for ensuring that all data that are made available to and used in the HBP comply with ethical and legal requirements rests with the Data Contributor who makes the data available. They need to:

1. Provide information about the Ethics authority which approved the research undertaken and the ID number of the approval, confirm that the research complies with EU ethics principles, and that they are willing to undergo an ethics audit (see Ethics compliance, below).
2. Upload their data to HBP storage, provide metadata, and undergo data curation (see Data registration, below).
3. Give permission for the use of the data by choosing a licence for the sharing of data (see Data licensing, below), and decide on a possible embargo period before public release.

Where the Data Contributor is not an HBP PI, they need to be sponsored by an HBP PI who accepts responsibility for ensuring that the conditions are met.

2.2. HBP storage and KnowledgeGraph

HBP storage is the persistent data storage provided by the HBP digital infrastructure service providers.

KnowledgeGraph is the provenance based metadata database provided by HBP digital infrastructure service providers.

Data Contributors are provided with information about how to upload their data to HBP storage and how to provide metadata. This process is facilitated by the HBP Data Curation Team.

Data in HBP storage is either open access, under a defined license (see below), or under embargo with access for selected researchers only, as determined by the Data Contributor.

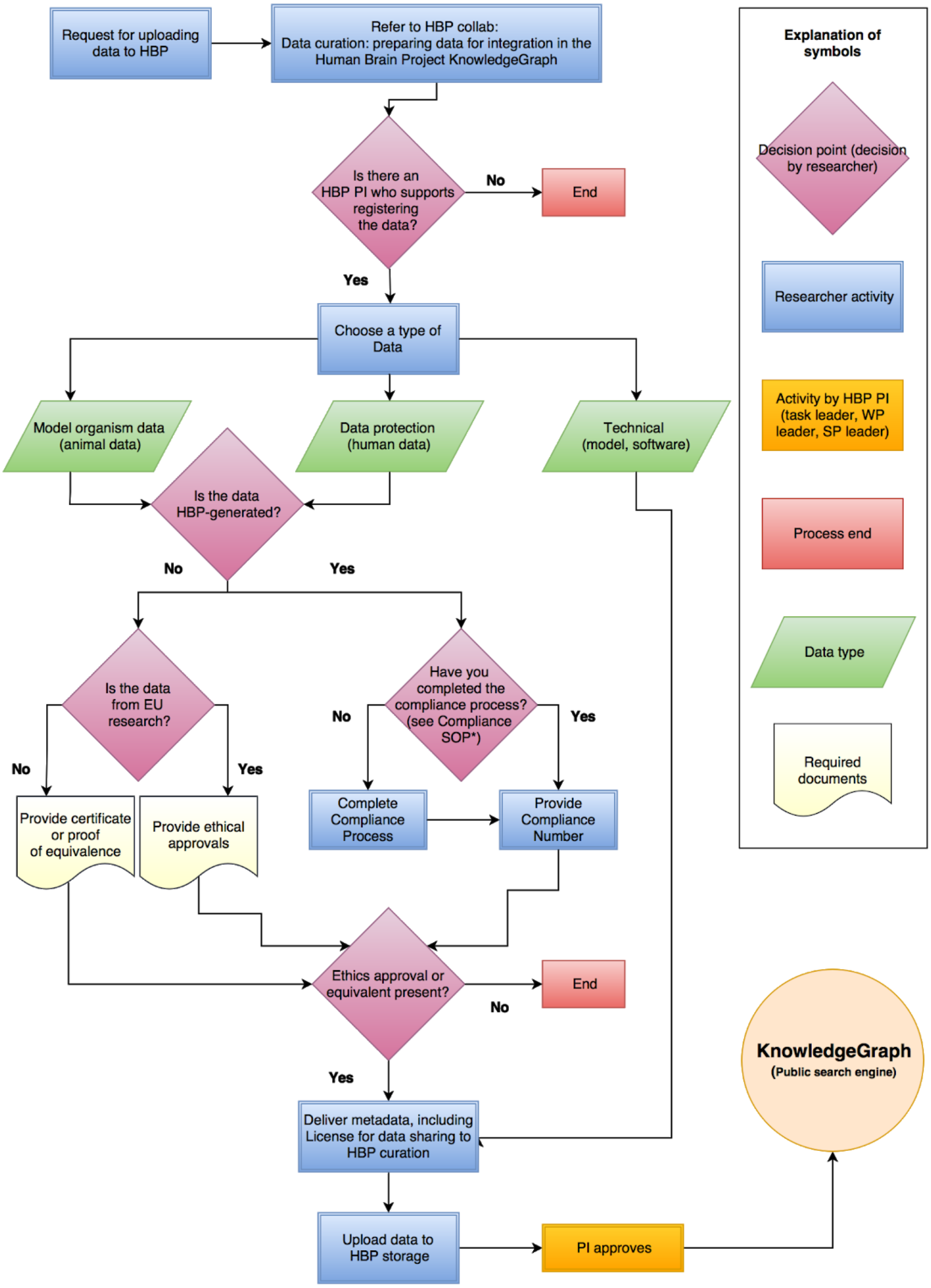
Metadata for data stored in HBP storage will be stored in the HBP KnowledgeGraph. All metadata in the HBP KnowledgeGraph are openly searchable.

2.3. Data Registration

Data registration is the process by which data are made accessible to/via HBP storage and KnowledgeGraph, below referred to as the HBP digital infrastructure.

The following flowchart gives an overview of the steps required to register data with the HBP:

Flowchart for registering data with Human Brain Project


Request for uploading data to HBP
Refer to HBP collab: Data curation: preparing data for integration in the Human Brain Project KnowledgeGraph
Is there an HBP PI who supports registering the data?
No
End
Yes
Choose a type of Data
Model organism data (animal data)
Data protection (human data)
Technical (model, software)
Is the data HBP-generated?
No
Yes
Is the data from EU research?
No
Yes
Provide certificate or proof of equivalence
Provide ethical approvals
Have you completed the compliance process? (see Compliance SOP*)
No
Yes
Complete Compliance Process
Provide Compliance Number
Ethics approval or equivalent present?
No
End
Yes
Deliver metadata, including License for data sharing to HBP curation
Upload data to HBP storage
PI approves
KnowledgeGraph
(Public search engine)
Explanation of symbols
Decision point (decision by researcher)
Researcher activity
Activity by HBP PI (task leader, WP leader, SP leader)
Process end
Data type
Required documents

Before data can be accepted by and made accessible via the HBP digital infrastructure, they need to be cleared to ensure compliance with ethical and legal requirements.

To make data visible to services comprising or connected to the HBP digital infrastructure, they must be registered in an index which is presently developed and maintained by the Neuroinformatics Platform. The registration process ensures that:

- Data are cleared to ensure compliance with ethical and legal requirements
- Data are annotated with metadata, based on ontologies or controlled vocabularies, to the extent that this is possible.
    - In cases where this is not possible, HBP digital infrastructure service providers will make an effort to ensure that newly produced ontologies are created/maintained at a level that is equivalent with established services in the biomedical research community.
- Data are serialized in a format that is registered in a data format index.
    - To ensure data remains accessible after it has initially been made accessible, HBP maintains a list of serialization formats. The addition of data formats will be possible during the registration process.
- Possible uses and reuse of the data are expressed via the use of well documented licenses and embargo.
    - All data shared through the HBP digital infrastructure services should be annotated with a license describing the conditions for use. The Data Contributor decides on the license that should apply from a list of licenses accepted by the HBP (see below) and whether or not an embargo period shall be imposed before release.

2.4. Ethics compliance (animal data)

- For data sourced from animal studies commissioned by/financed through the HBP, the Data Contributor confirms that the data was collected in research that complied with:

    - Ethical principles as outlined by the Horizon 2020 Ethics Self-Assessment[3]
    - Applicable international, EU and national law (in particular, EU Directive 2010/63/EU)[4].
    - Where the research was undertaken in an EU Member State with stricter rules, these were adhered to.
    - The research favoured alternatives to animal use, and implemented the principles of replacement, reduction and refinement (‘three Rs’).
    - If the data included Non-human primates (NHPs), the Data Contributor is aware of the special conditions linked to this.
    - The use of great apes requires very exceptional justification, and must be specifically authorised by the Commission/Agency.
    - The above conditions are normally considered to be met, if the research is covered by a valid ethics approval from a competent authority within an EU Member State.

- For data re-used from animal studies conducted outside of the scope of HBP/without funding from HBP:

    - Data that is sourced from facilities which have proven compliance with the US ILAR Guide for the Care and Use of Laboratory Animals[5] may be used. This Guide is a set of standards which are well accepted internationally and govern the housing, care and treatment of laboratory animals. For rodents, they are considered a globally acceptable standard. Such compliance can be substantiated by an AAALAC (Association for Assessment and Accreditation of Laboratory Animal Care) accreditation, or by a publication in an international tier 1 peer-reviewed journal that endorses the ARRIVE guidelines.[6]

    - In cases where the above can not be guaranteed due to unresolvable historic provenance gaps (e.g. some bioinformatics data in public databases) registration of data may still be possible, but requires approval by the HBP via an audit.

[3]http://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-msca-itn-2015/1620147-h2020_-_guidance_ethics_self_assess_en.pdf

[4] This Directive aims at limiting the use of animal testing for scientific purposes and provides for common standards for the welfare of animals that are used (including authorisations, restrictions for the use of certain kinds of animals, standards for procedures, minimum requirements for personnel, recording and traceability, care and accommodation).

[5] https://grants.nih.gov/grants/olaw/Guide-for-the-Care-and-use-of-laboratory-animals.pdf, accessed 23.08.2016

[6] https://www.nc3rs.org.uk/arrive-animal-research-reporting-vivo-experiments#journals, accessed 17.08.2016

- The Data Contributor is willing to comply with an audit by the HBP and provide the above evidence to the HBP within 2 weeks of receiving a request.

- The Data Contributor is aware that failure to provide relevant evidence to an HBP audit can lead to the removal of the data from the HBP systems, the closing of their user account, and a notification of their institution's ethics bodies concerning potentially unethical practice.

Data Contributors need to confirm that they have evidence to demonstrate the compliance of their data with these principles. They will be asked to provide the details of the competent authority that gave approval for the research and use of data as well as an approval number. They will accept audit procedures and provide detailed information and documentation. For further guidance, it is recommended that Contributors consult the HBP SOP on Animal Data[7].

2.5. Data Licensing

This section addresses HBP policy for data licensing. While software can be considered data, this section ignores software licensing policies.

All data registered with the HBP needs to be licensed for further use by the owner. The Data Contributor must choose during the process of registration which licence is appropriate and will be used to make the data available. The HBP allows users to choose any Creative Commons version 4.0 licence[8]. The default option is the most open licence, CC-BY. The Creative Commons licenses below have been selected for their compatibility with the FPA-CA.

The Data Contributor may choose to impose an embargo on the access to data. In the embargo period, only selected researchers, as determined by the Data Contributor, have access to the data.

The resulting choice of licences is as follows:

	Do you allow commercial uses of your work?	
	Yes	No

[7] https://sos.exo.io/public-website-production/filer_public/c4/40/c440fd2b-59c2-411c-983b-8faa1426c14c/updated_m18__sga1_d1242_d715_d2_animal_data__third_countriesrequirement_no_5.pdf

[8] https://creativecommons.org/choose/

Do you allow adaptations of your work to be shared?	Yes	Attribution 4.0 International cc BY (this is the default)	Attribution-NonCommercial 4.0 International cc BY NC
	No	Attribution-NoDerivatives 4.0 International cc BY ND	Attribution-NonCommercial-NoDerivatives 4.0 International cc BY NC ND
	Yes, as long as others share alike	Attribution-ShareAlike 4.0 International cc BY SA	Selected License Attribution-NonCommercial-ShareAlike 4.0 International cc BY NC SA

3. EU Data Protection Law and the HBP

In the EU, data protection and privacy receive high legal standing as expressed in the Charter of Fundamental Rights in the European Union. During the lifetime of the HBP, the longstanding Data Protection Directive[9] was replaced by the General Data Protection Regulation (hereinafter 'GDPR'[10]). The GDPR is applicable to the HBP from 25 May 2018. There is no 'grace' period, and all aspects of the HBP must be compliant by that date.

The GDPR is designed to harmonize EU data protection law and apply equally or uniformly across all EU member states. Like the Directive it replaces, the GDPR is a complex

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 31–50 ('95/46/EC' or 'the Directive').

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. The GDPR shall apply from 25 May 2018. GDPR Art. 99(2).

principle-based legislative instrument containing derogations and room for interpretation in many areas. As further interpretations become available, the DPM will be updated to reflect those changes.

3.1. Material Scope and Application of European Data Protection Law

3.1.1. Personal Data

The GDPR only applies to personal data. This is defined broadly to include *"any information* relating to an identified or identifiable natural person." The GDPR also regulates sensitive personal data, which includes genetic data and biometric data processed to uniquely identify an individual, as special categories of data. These special categories of data have additional legal requirements.

The GDPR does not apply to fully anonymized data, data concerning deceased persons, or data used for solely 'household purposes.'

In general, most data collected and processed in the HBP regarding human subjects will be considered personal (e.g. MRIs, blood samples). Additionally, 'any information' is broad enough to also include questionnaires and case studies in addition to registries. Registries for access including identification material (e.g. copy of a passport) is also personal data and data processing must comply.

3.1.2. Anonymized Data

If data is fully anonymized, it is no longer considered to be personal and is thus outside the scope of GDPR application. In other words, if HBP data is fully anonymous the GDPR does not apply. However, given the difficulty in creating truly anonymous data, the bar for anonymization has been set extremely high in the EU. Although there is no prescriptive standard for anonymization in the EU, the WP29 states that fully anonymized data requires "irreversibility preventing identification of the data subject" taking into account all the means "reasonably likely to be used" for identification. In short, effectively using this exception in practice is extremely difficult.

3.1.3. HBP Policy

If HBP human data requires re-identification at some point, the data is not fully anonymized for purposes of the GDPR. The GDPR will remain applicable. Personal data that have been pseudonymised (i.e. encrypted) has certain advantages under the GDPR such as data breach reporting. Whenever possible, HBP data should be pseudonymised. However, the GDPR applies to pseudonymised data.

3.2. Data Processors and Data Controllers: Roles and Responsibilities

Two of the most important roles in EU data protection law are that of data 'processor' and data 'controller.' The controller/processor relationship largely boils down to an allocation of responsibility. Under the GDPR, data controllers have the primary responsibility for treating the personal data entrusted to them in a way which conforms with the law.

The primary component necessary to meet the controller designation is that the natural or legal person makes a specific determination regarding 'the purposes and means' of data processing. If the 'purpose and means' of processing is determined by various entities working in concert, they may be considered 'joint controllers' where responsibility is shared. The GDPR places requirements on parties based on their actual roles in data processing operations and not simply the labels they give themselves.

3.2.1. HBP Policy

In the HBP, hospitals determining 'the purposes and means' of data processing will be considered controllers of patient data. If the HBP determines 'the purposes and means' of the processing of data stored on its platform, it will also be considered a controller.

In certain cases HBP partners act on instructions of the HBP and use HBP software and systems under the control or management of the HBP. Because the HBP determines the 'purposes and means' of processing of personal data on its platforms, it may be considered a controller. As such, the HBP would be required to comply with all controller requirements in the GDPR. The HBP will in many cases have joint responsibilities with other controllers. The detailed analysis of the distribution of responsibilities will need to be undertaken in SGA2 when data that is subject to the GDPR will be used by central HBP systems and the joint platform.

3.3. Lawful Processing Personal Data

The GDPR broadly requires a legal basis for *any* processing of personal data. For processing to be lawful, the processing party must have legitimate grounds for the entire duration of the processing. The basis for processing of personal data must be determined at the beginning of processing, and there is little flexibility for amendment after processing has begun. In the

HBP, consent is widely used as a legal basis for data processing, although other bases are possible.

3.3.1. Consent

In some cases, the same legal basis may be used to cover multiple processing operations. A legal basis applicable in one situation will not necessarily be appropriate or available in all others. For example, a core requirement of consent is that it be freely given and contain an element of genuine choice. In some situations, the imbalance of power is so great that consent will not be valid. This is the case with both public authorities and employers. In the HBP, this could potentially be an issue where consent to research is provided in the context of treatment.

3.3.2. Consent by Children

The GDPR limits the age at which consent can be given by an individual. The HBP will therefore have to employ mechanisms to determine the age of users—and if they are under the age of 13—obtain the requisite consent from parents or legal guardian so that processing may lawfully take place.

3.3.3. Consent and Sensitive Personal Data

If the data being processed is sensitive personal data, including medical records, additional requirements must be met. For example, explicit consent is required. Many of the HBP SPs will process sensitive personal data. Therefore, they must have in place a process to obtain specific consent and further demonstrate that such consent has been obtained prior to processing.

3.3.4. HBP Policy

Processing of personal data requires a legal basis, which must be determined before processing. In the HBP, that basis will often be consent. The HBP has developed a Standard Operating Procedure on informed consent, available on the ethics resources webpage[11].

[11] http://www.humanbrainproject.eu/en/social-ethical-reflective/ethics-resources/ethics-resources/

3.4. Principles relating to the processing of personal data

The GDPR Principles relating to processing of personal data are fundamental to compliance with data protection law. In addition to applying the principles, HBP partners must be able to demonstrate compliance with the principles through documentation.

3.4.1. Data must processed fairly, lawfully, and transparently

For processing to be **lawful**, HBP partners must follow the legal requirements set out in the GDPR, in addition to other instruments such as contracts or codes of conduct.

Fairness requires that the party processing personal data (e.g. the controller or processor) does not act unreasonably, and takes into account the interests and rights of the data subject. Repurposing, selling, or reusing data in a way that exceeds the consent provided by the data subject is clearly unfair.

In the HBP context, **transparency** requires that the controller provide the data subject (e.g. a patient) with adequate and accurate information regarding the basis for the processing, the extent of the processing, and the data categories or recipients with access to the data.

3.4.2. Purpose limitation principle

This principle requires that the controller set a specific purpose for data processing *prior to* collection of personal data. Any further use of the data collected must also remain compatible with the original purpose. After choosing a purpose, the processing of personal data that follows must necessarily fulfill that purpose. Any further use of the data collected must also remain compatible with the original purpose.

If data is processed in a manner incompatible with the purpose for which it was initially obtained, the processing is unlawful. In the HBP, a clear violation of this principle is using data collected for medical research and repurposing that data for advertising purposes or other acts beyond the consent of the data subject.

3.4.3. Data minimization

In addition to attaching a specific purpose to data collection, the principle of data minimization requires that data collected be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In the HBP, this means if the data used for research only requires an MRI, collecting additional medical or other personal information must be avoided. Along with purpose specification, this principle poses particular challenges for big data analytics.

3.4.4. Data Accuracy and Quality

EU data protection law also requires that data be "accurate and, where necessary, kept up to date." If data is no longer accurate, the data must be erased or corrected.

3.4.5. Storage limitation

In addition, even where the data is accurate and up to date, it should not be kept in a form that identifies the data subject for "…longer than is necessary for the purposes for which the personal data are processed…[]." Retention periods may vary depending on the purpose of the initial collection.

3.4.6. Confidentiality and integrity principle

Personal data must be handled "…in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage…". Although encryption is an important security aspect, re-identification is possible using a key. Therefore, the processes lacks the 'irreversibility' required to render the data non-personal or fully anonymous. Consequently, encrypted data is not anonymous data, and EU data protection requirements remain applicable. However, pseudonymisation of data through encryption or by other means (e.g. hash function, tokenization) contributes to meeting this principle in the HBP.

3.4.7. Accountability principle

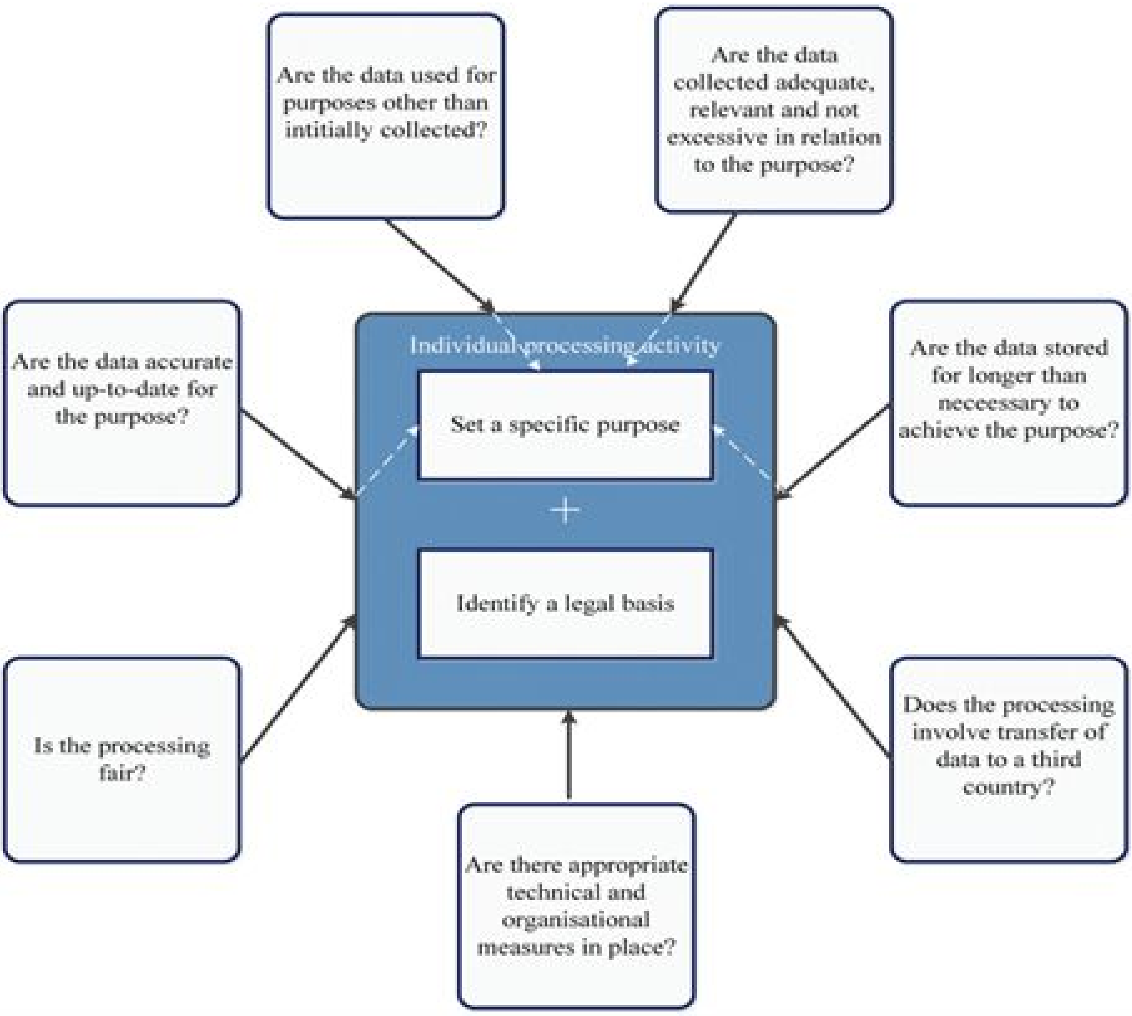
The above principles remain consistent between the Directive and the GDPR. However, under the GDPR, the controller is now required to "…demonstrate compliance…" with the above principles. To meet this principle, HBP partners will be required to document their compliance with the above principles.

3.4.8. Summary and HBP Policy:

Controllers in the HBP must:

- Implement and apply the above data protection principles, and
- Demonstrate compliance with the principles through documentation

The table below visually demonstrates the application of these principles[12]. The first step requires setting a specific purpose for data processing (e.g. ‘medical research’). The second is identifying a legal basis (e.g. ‘explicit consent’). Based on the purpose, the controller (defined below) should be able to account for and answer all the questions demonstrating the data protection principles in the boxes surrounding purpose and processing actively.


Are the data used for purposes other than intitially collected?
Are the data collected adequate, relevant and not excessive in relation to the purpose?
Are the data accurate and up-to-date for the purpose?
Individual processing activity
Set a specific purpose
+
Identify a legal basis
Are the data stored for longer than neceessary to achieve the purpose?
Is the processing fair?
Does the processing involve transfer of data to a third country?
Are there appropriate technical and organisational measures in place?

[12] From Esayas 2017, pg. 142 https://academic.oup.com/ijlit/article/25/2/139/2998971

3.4.9. Derogations for scientific research (Art. 89, Rec. 33, WP29 Opinion)

Pursuant to GDPR Article 89, where personal data are processed for scientific or historical research purposes or statistical purposes, a Union or Member State law may provide for derogations from the rights referred to in Articles 15 (Right of access by the data subject), 16 (Right to rectification), 18 (Right to restriction of processing) and 21 (Right to object) subject to certain conditions and safeguards. Derogations must be necessary for the fulfilment of the scientific research purposes. As a result, this is an area that will vary among EU member states.

Currently, most member states are reviewing or drafting derogations for scientific research. When more information becomes available, the DPM will be further updated.

3.5. Data Processing Agreements and the HBP

Specific controller requirements under the GDPR include choosing a data processor that provides "sufficient guarantees" regarding their ability to meet legal requirements, and implements "appropriate technical and organizational measures." Further, a data processing contract or other binding agreement that specifies processor compliance requirements is also compulsory. Contractual obligations under the GDPR include:

- The processor processes the personal data only on documented instructions from the controller (including terms on subject matter, duration, nature of the processing, type and categories of data).
- The processor's commitment to confidentiality requirements.
- The processor follows security measures as required per GDPR Art. 32.
- The processor only engages a subprocessor with "prior specific or general written authorisation of the controller."
- The processors must also assist the "controller in ensuring compliance with the obligations" including security, data breach, and Data Protection Impact Assessments (DPIAs).
- The processor "deletes or returns all the personal data to the controller" after the relationship ends.
- The processor makes information available to the controller to assist with audits and inspections.

All contracts entered into with processors, such as cloud service providers, must contain the above terms in a data processing contract. Additionally, cloud computing services can only be used if they have been vetted with the following procedure:

- Verify the existence of a compliant Privacy Policy.
- Verify the compliance of the service with the GPDR via Privacy Shield or similar mechanism of verified adequacy (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pd)
- Document this information and any other relevant information using the HBP Cloud Provider GDPR Compliance Report.
- Ensure the data processing agreements meets the requirements outlined above (i.e. from GDPR Article 28).

3.6. Individual Rights

HBP partners must support compliance with individual rights when applicable including:

- The right to be informed (GDPR Arts. 13-14)
- The right of access (GDPR Art. 15)
- The right to rectification (GDPR Art. 16)
- The right to erasure ('right to be forgotten') (GDPR Art. 17)
- The right to restrict processing (GDPR Art. 18)
- The right to data portability (GDPR Art. 20)
- The right to object (GDPR Art. 21)
- Rights in relation to automated decision making and profiling (GDPR Art. 22)

3.7. Accountability, governance, and data security

3.7.1. Data Protection Officer (DPO)

The HBP appointed a Data Protection Officer (DPO) in 2017 after a proposal by the Ethics Management group to the SIB and DIR. The DPO will report to the Director General.

The role of DPO includes consultation on data processing activities and providing advice and recommendations on compliance with applicable laws. In particular, the DPO assists in carrying out data protection impact assessments (DPIA), among other compliance tasks.

In addition to data protection compliance, the DPO has a communication function and consults with data subjects, HBP partners and leadership, and supervisory authorities. To contact the HBP DPO, please fill out this form[13].

3.7.2. Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is a tool for building and demonstrating compliance with the GDPR. A DPIA is an ongoing process that should "be continuously reviewed and regularly re-assessed." This is particularly necessary when adding new technologies (e.g. the Medical Informatics Platform). A DPIA should take place "prior to the processing" of personal data.

As controller, the HBP is required to conduct a DPIA. In conducting a DPIA, the HBP must consider the context and types of data being processed, the legal requirements it has regarding data under the GDPR, assess privacy risks associated with HBP processing activities, and apply a method to treat or address risks. If the risks cannot be adequately addressed, the HBP will petition the supervisory authority for further guidance.

A separate opinion on a DPIA at the level of the HBP, including methodology and process, is in development.

3.7.3. Data protection by design and default

Data protection by design and data protection by default require that ICT systems safeguard the rights of data subjects. Compliance requires integration of technical and organizational measures such as pseudonymisation and data minimisation. Technical measures should be the 'default' setting and limit the amount of data collected, the extent of processing, and access to personal data.

The HBP will formulate and apply technical and organisational, measures to enhance privacy by design in developing information platforms to share data for research purposes. This will be facilitated through the modelling of data flows. This will be contextualised via a risk-based assessment in order to ensure proportionate responses are developed for different areas of activity. These measures will be 'baked in', not added on, to policy and infrastructure development. The impacts will be in terms of data collection, use, retention, and destruction, including a purpose-based minimisation of activities which enshrines the obligation for privacy by default.

[13] https://skjema.uio.no/94779

All HBP SPs and partners are required to design, develop, and operate their services employing “privacy by design” and “privacy by default” principles.

3.7.4. Data Security

The HBP is committed to the confidentiality and security of personal and other data stored with the project. HBP data must be encrypted when ‘in transit’ and, when available, to data ‘at rest.’ HBP partners are required to follow industry standard methods and best practices for cryptographic key management. Examples of acceptable encryption protocols include SSL or SSH, with appropriate key generation techniques and key lengths.

All administration of HBP systems must use secure communications channels. Other security measures, including strong authentication measures, must also be imposed whenever possible. Further, all HBP providers and their subcontractors must commit contractually to meet all HBP confidentiality and security obligations.

A separate document detailing current HBP policies (i.e. encryption, security patches, audit, and storage) is currently in development.

3.7.5. Data Retention Policy

Any dataset used to produce a scientific result or infrastructure service under the Ramp-up or Operational Phase of the HBP is subject to the standard EC data retention conditions. It must remain available, at least within an Archival-class data repository, for 5 years after the end of the Operational Phase of the HBP, as defined in the FPA-CA. This then places a financial burden on any site hosting data for periods of time that extend beyond the end of the Operational Phase of the HBP, and these need to be appropriately accounted for and provisioned in such a way as to permit compliance with said regulations

3.7.6. Data Breach Notification

Where a data breach has been identified or is suspected by any user of HBP systems involving or suspected to involve data produced or owned by the HBP through its partners, this should be notified by submitting it to the Point of Registration system. This should be done via the PORE mechanism[14].

A submission should include at least the following information

1. Name of the reporting individual and means of contacting them (email)
    a. Anonymous submissions are possible but not encouraged.

[14] http://www.hbp-pore.eu/

2. Nature of the data breach
    a. Dataset affected
    b. Cause of breach
    c. Description of breach
3. Description of how it was identified
4. Information about breaches to HBP management

Upon submission to the PORE registrar, the data breach will be brought to the attention of the Ethics Manager and Ethics Management team.

An immediate notification will be sent to the DIR.

Where required, further investigations will be undertaken to clarify the exact nature of the breach and its consequences.

Ethics Management and the DIR will identify the relevant supervisory authority and report the breach to this authority.

3.8. Legal Liability

Violation of the GDPR may result in administrative or other sanctions. Depending on the violation, maximum GDPR fines range from 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover up to 20 000 000 EUR, or (also in the case of an undertaking), up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. As controller, the HBP may subject to the largest fine, depending on the nature of the violation.

3.8.1. HBP Policy

Infringements may be identified during an audit, via the HBP reporting mechanisms or via an external event. Where administrative fines or other sanctions are to be paid, the shared responsibility will be determined by the HBP Directorate in collaboration with the affected partners. If an agreement cannot be reached, the Ombudsperson may be involved to facilitate a resolution, though co-responsibilities may be settled in court under the GDPR. At the time of writing, the HBP Ombudsperson is Professor Krista Varantola.

4. References

- HBP Data Policy Manual (unpublished, available upon request from hbp.compliance@dmu.ac.uk)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (hereinafter 'GDPR'), available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 31–50 ('95/46/EC' or 'the Directive'). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL
- EU Directive 2010/63/EU
- Samson Y. Esayas; The idea of 'emergent properties' in data privacy: towards a holistic approach, International Journal of Law and Information Technology, Volume 25, Issue 2, 1 June 2017, Pages 139–178, https://doi.org/10.1093/ijlit/eaw015