

Project Number:	785907	Project Title:	Human Brain Project SGA2
-----------------	--------	----------------	--------------------------

Document Title:	D12.4.1 - Data Policy Manual
Document Filename:	D12.4.1 (D78.1 D114) SGA2 M1 ACCEPTED 190723
Deliverable Number:	D12.4.1 (D78.1, D114)
Deliverable Type:	Report
Work Package(s):	All SPs
Dissemination Level:	PU = Public
Planned Delivery Date:	SGA2 M01 / 30 APR 2018
Actual Delivery Date:	SGA2 M1 / 30 APR 2018, Resubmitted M13 12 APR 2019; ACCEPTED 23 Jul 2019

Authors:	Data Governance Working Group, with substantial contributions by: Kevin MCGILLIVRAY UIO (P81), Bernd STAHL DMU (P16), Martin TELEFONT EPFL (P1), Katrine ORE UIO (P81), Jeff MULLER EPFL (P1), Jan BJAALIE UIO (P81), Colin MCMURTRIE ETHZ (P18), Tyr FOTHERGILL DMU (P16)
Compiling Editors:	Bernd STAHL DMU (P16), Tyr FOTHERGILL DMU (P16)
Contributors:	SP12, Ethics Advisory Board
SciTechCoord Review:	##
Editorial Review:	Annemieke MICHELS, EPFL (P1)

Abstract:	<p>This Deliverable is submitted to address the following requirement: Having a set of data-related policies is a requirement for the HBP in order to:</p> <ul style="list-style-type: none"> <li>- Ensure that expectations with regards to data handling are clear - Comply with all data-related regulations and legislation, in particular those related to data protection</li> <li>- Ensure that all data registered and used in the HBP comply with ethical and other requirements</li> <li>- Demonstrate good management and leadership and implement good practice in data management.</li> </ul>
Keywords:	Data Governance, Data Protection, Compliance

Target Users/Readers: Consortium members

A Live version of the Data Policy manual for HBP members can be found here:

<https://collab.humanbrainproject.eu/#/collab/34766/nav/241033>

## Document Approval Status

Date	Comments
30.03.2017	Initial draft
30.11.2017	First complete draft
15.12.2017	Internal review of parts I, II, and III complete
15.01.2018	Revision by section authors, members of Data Governance Working Group
30.01.2018	Internal review of parts IV and V complete
01.02.2018	External review of parts I, II, and III complete
28.02.2018	External review of parts IV and V complete
16.03.2018	Revision of entire manual by section authors, members of Data Governance Working Group
26.03.2018	Preparation for submission at the end of SGA1
01.08.2018	SGA2 Revision following SGA1 Ethics Review
17.10.2018	The DMP was presented to the EAB at the HBP Summit in Maastricht in October 2018. The EAB was positive to the development, but expressed that they did not have the time or expertise to approve the DPM.
21.01.2019	Approval by SIB
04.02.2019	Approval by DIR
12.04.2019	Resubmitted to European Commission following revisions and approval by SIB and DIR



## Table of contents

<b>1. Introduction .....</b>	<b>5</b>
1.1 Structure and Purpose of the Data Policy Manual .....	6
1.2 Abbreviations and Acronyms .....	6
1.3 Definitions .....	7
<b>2. Classification of Data and Resulting Requirements .....</b>	<b>9</b>
2.1 Types of Data .....	9
2.2 Ethical Requirements Based on Source Organism.....	9
<b>Part I .....</b>	<b>11</b>
<b>3. Data Protection Guidance and Policy in the HBP.....</b>	<b>11</b>
3.1 Application, terminology and Icons .....	11
3.2 Data Protection Law in the EU .....	13
3.3 Risk-Based and Scalable Approach to the GDPR .....	13
3.4 Material Scope and Application of European Data Protection Law: Processing of Personal Data	13
3.4.1 Personal data in the HBP .....	14
3.4.2 Special categories ('sensitive') personal data .....	16
3.4.3 Territorial Application of the GDPR to the HBP .....	18
3.5 Data Processors and Data Controllers: Roles and Responsibilities.....	18
3.5.1 Data Controllers in the HBP .....	19
3.5.2 Data processors in the HBP.....	20
3.6 Data processing agreements and SP Controllers .....	21
3.7 Principles Relating to Data Quality and Application to the HBP .....	22
3.7.1 Data must be processed fairly, lawfully, and transparently.....	22
3.7.2 Purpose specification and limitation principle .....	23
3.7.3 Data minimisation.....	24
3.7.4 Data accuracy and quality .....	24
3.7.5 Storage limitation and deletion: .....	25
3.7.6 Integrity and Confidentiality .....	26
3.7.7 Accountability principle.....	27
3.7.8 Accountability in the HBP .....	27
3.8 Legal basis for lawful Processing of Personal Data .....	29
3.8.1 UK ico PrivacyPolicy .....	32
3.9 Scientific Research .....	32
3.9.1 General application of the GDPR to scientific research.....	33
3.9.2 Legal Basis for Scientific Research.....	33
3.10 Consent in Scientific Research .....	34
3.10.1 Consent in research.....	34
3.10.2 Impact on Broad Consent .....	36
3.10.3 Withdrawal of consent .....	36
3.11 Relevant Scientific Research (SR) Derogations by Member State .....	37
3.12 Data protection by design and default .....	40
3.13 Individual Rights .....	41
3.13.1 The right to be informed .....	42
3.13.2 The right of access.....	43
3.13.3 The right to rectification .....	43
3.13.4 The right to erasure ('right to be forgotten').....	44
3.13.5 The right to restrict processing.....	44
3.13.6 The right to data portability .....	45
3.13.7 The right to object.....	45
3.13.8 Rights in relation to automated decision making and profiling.....	46
3.14 Data Protection Officer .....	46
3.15 Documentation Requirements.....	48



3.16	Data Breach .....	48
3.17	Data Protection Impact Assessment (DPIA) .....	50
3.17.1	Carrying out a DPIA: Methodology.....	51
<b>4.</b>	<b>Data Anonymisation.....</b>	<b>53</b>
<b>5.</b>	<b>International data Transfers .....</b>	<b>56</b>
5.1	Privacy Shield .....	56
5.2	Appropriate safeguards.....	57
5.2.1	Standard contractual clauses .....	57
5.2.2	Binding corporate rules .....	57
5.3	Derogations .....	57
<b>Part II: Data Contribution and Model Organism Data (Animal Data) .....</b>		<b>59</b>
<b>6.</b>	<b>Model Organism Data .....</b>	<b>59</b>
6.1	Data Contributors .....	59
6.2	HBP storage and Knowledge Graph.....	60
6.3	Data Registration .....	60
6.4	Ethics compliance (animal data) .....	62
6.5	Data Licensing.....	63
<b>DPM Inventories and Worksheets .....</b>		<b>65</b>
Inventory I: Controller/SP Documentation Worksheet .....		65
Inventory II: DPIA Template .....		70
Inventory III: Data Protection by Design and Data Protection by Default .....		70
Inventory IV: General Security of Personal Data Inventory .....		70

## 1. Introduction

The Human Brain Project (HBP) is developing an ICT infrastructure for neuroscience. The HBP is centrally concerned with the collection, analysis, and dissemination of a broad range of different types of data. In addition to the scientific challenges that this work raises, ethical challenges and issues of legal rights and obligations are also present. As a highly visible and publicly funded European project, the HBP must demonstrate compliance with legislation and show an active engagement with good practice and the state of the art. As a world-leading project, the HBP has the ambition to be at the forefront of questions of international collaboration in ICT and neuroscience and to develop standards in the use and exchange of data. This Data Policy Manual (DPM) expresses the policies that the HBP has developed to realise these ambitions.

In more detail, 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.
- Implement standards for demonstrating compliance and accountability through Data Protection Impact Assessments (DPIAs) and other tools.
- Ensure that all data registered and used in the HBP comply with ethical and legal requirements.

The policies outlined in this document were prepared by the Data Governance Working Group and adopted by the DIR and SIB.

This document further aims to reconcile ethical and legal requirements with the [FAIR Guiding Principles for scientific data management and stewardship](#) and implementation-level policies described in the [Research Data Alliance \(RDA\) Practical Policy](#) document. This RDA document recommends defining the following minimum policies:

- 1) Contextual metadata extraction policies (if any)
- 2) Data access control policies
- 3) Data backup policies
- 4) Data format control policies (if any; will be optional, many data repositories will be format agnostic)
- 5) Data retention policies (must be supported by the Terms of Service for the data repository)
- 6) Disposition/Data lifecycle and archiving policies
- 7) Notification policies
- 8) Restricted searching policies
- 9) Storage cost policies
- 10) Use agreement policies

The DPM refers to all data used and collected in the HBP and is intended to be a standard-setting document throughout the HBP. Whilst the use of data in and through the NIP (Neuroinformatics Platform) is a primary focus, the policies are in most cases comprehensive insofar as they are relevant to universal structures with which the HBP must comply (e.g. the EU General Data Protection Regulation and other legislation). In some areas, the HBP may create and define

additional processes that may exceed the requirements outlined in this document in a ‘beyond compliance’ approach. However, the DPM provides an essential baseline to be applied across the project.

## 1.1 Structure and Purpose of the Data Policy Manual

A core thread running through the HBP is compliance with all applicable domestic, European, and international regulations concerning data. Depending on whether data are human or animal, different regulatory requirements attach or apply. The point of departure and purpose of the DPM is to provide a description of the relevant HBP policy for use by HBP partners and scientists. The DPM is a ‘living document’ and will be subject to changes and updates as new policies are adopted or legal requirements change.

Abbreviations, definitions, and the process for categorising data and the relevant requirements or obligations are outlined in the sections below. These are followed by a flow chart for analysing many of the issues faced in the HBP.

In [Part I](#), the DPM evaluates EU data protection law and as it applies to the HBP. In short, applying the General Data Protection Regulation to the HBP is complex. Furthermore, obligations under the GDPR will vary considerably for some HBP partners. The point of departure is to provide guidance and set ‘global’ standards that will serve as a starting point for increasing accountability and GDPR compliance throughout the project.

Research requirements for human research that go beyond data protection are also included in this section. This aspect of the DPM is currently being updated.

In [Part II](#) Part II: Data Contribution and Model Organism Data (Animal Data), the DPM focuses on principles and requirements related to model organism data (animal data). This section also provides an overview of data entry into the Neuroinformatics Platform (NIP).

## 1.2 Abbreviations and Acronyms

API	Application Programming Interface
DPO	Data Protection Officer
DIR	Directorate, one of the governing bodies of the HBP
DPIA	Data Protection Impact Assessment
FPA	Framework Partnership Agreement
GDPR	General Data Protection Regulation
HBP	Human Brain Project
MIP	Medical Informatics Platform
NIP	Neuroinformatics Platform
PI	Principal Investigator
PIA	Privacy Impact Assessments

RUP	Ramp Up Phase
SGA1	Specific Grant Agreement 1
SGA2	Specific Grant Agreement 2
SIB	Science and Infrastructure Board, the main scientific body of the HBP, which is comprised of the SP leaders and a representative of the Partnering Projects
SOP	Standard Operating Procedure
SP	Sub-project, fundamental components of the HBP entitled by broad area of research (e.g. “SP4: Theoretical Neuroscience”)
ToS	Terms of Service agreement

## 1.3 Definitions

The definitions provided below are generally applicable to the entire DPM. However, in some sections the definitions are expanded, for example if the definition is a ‘term of art’ and has a specific meaning in the context of a particular regulation. If there is a conflict between the terms below and guidance in a specific DPM section, users should rely on the more specific term provided in the section dedicated to the topic being evaluated (i.e. data protection or animal research).

Term	Definition
Anonymous data	Information which does not relate to an identified or identifiable natural person.
Consortium	Group of organisations that consist of all of the parties which are part of the HBP Agreements, but excluding the European Commission (EC).
HBP partner	Any party to the HBP Agreements, excluding the European Commission (EC)
Contributor	Individuals and/or institutions that produce and make available Datasets on the Platform to the Data Users
Contributor Registration	Process that allows Contributors to have access to HBP systems and services and make Datasets available.
Data and Dataset	Data is used broadly in the context of the DPM including human data, animal data, or data derived by technical work. Dataset is an identifiable collection of data, either raw or derived, and its associated metadata, including data and metadata derived from monitoring protocols, field observations, collections, laboratory analysis, camera trap images, as well as written, recorded, graphic, audiovisual or other materials in any media. A Dataset may contain software and algorithms.
<a href="#">Data Controller</a>	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Custodian	A natural or legal person, public authority, agency, or other body with a legal right or title to control of the data in question. For human data this will normally be the





	Data Controller. Historically this has also been called a Data Owner, but this term is problematic when considering human personal data in the frame of the GDPR.
<a href="#">Data Processor</a>	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Data Producer	A natural or legal person who collects data as part of their working duties. Under their contract, they relinquish some or all of their title to a Data Custodian, typically their employer.
<a href="#">Data Protection Officer (DPO)</a>	The DPO is a professional in the field of data protection and assists with monitoring of internal compliance and data protection obligations across the HBP.
Data Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
Data User	A natural or legal person who accesses data.
Dual Use	Concerns research involving goods, software, and technologies covered by the EU export control Regulation No 482/2009. Dual Use items are normally used for civilian purposes but may have military applications, or may contribute to the proliferation of weapons of mass destruction.
HBP	The Human Brain Project under the FET Integrated Project (FP7 Grant Agreement no. 604102, i.e. its ramp-up phase), and its subsequent continuation under Horizon 2020 (Framework Partnership Agreement n°650003, Specific Grant Agreement no. 720270, i.e. SGA1) and any following continuation of the project under Horizon 2020 or other instrument.
HBP Agreements	Agreements concluded in respect of the HBP, such as FP7 Grant Agreement no. 604102, the Consortium Agreement under the FP7 Grant Agreement no. 604102, the Framework Partnership Agreement no. 650003 and related Specific Grant Agreements (SGAs), the HBP-FPA Consortium agreement and their subsequent agreements if applicable.
Metadata	Data about data; describes features of Data or Datasets
Medical Informatics Platform (MIP)	The Medical Informatics Platform is a sub-project of the HBP consisting of a Global Open-Source Platform allowing hospitals and research centers worldwide to share medical data whilst strictly preserving patient confidentiality.
Neuroinformatics Platform (NIP)	The Neuroinformatics Platform is a sub-project of the HBP (SP5). It serves as the HBP's search engine for distributed data, curated data repositories, brain atlases, and knowledge about the brain. The Platform consists of APIs for querying and a web-based platform and application programming interface (APIs), i.e. a set of standards, protocols, and tools for building software applications.
<a href="#">Personal Data</a>	Data relating to an identified or identifiable natural person.
Platform	Systems in the HBP that focus work, research and data. HBP Platforms are historically linked to sub-projects. Platforms of the HBP include: <ul style="list-style-type: none"> <li>• Neuroinformatics Platform</li> <li>• Simulation Platform</li> </ul>



	<ul style="list-style-type: none"> <li>• High Performance Analytics and Computing Platform</li> <li>• Medical Informatics Platform</li> <li>• Neuromorphic Computing Platform</li> <li>• Neurorobotics Platform</li> </ul>
Principal Investigator	<p>An individual who represents a partner organisation in a senior role in the HBP. Typically a PI will be a task leader, work package leader, or sub-project leader. A partner organisation may have more than one PI. They are best placed to determine the scientific, technical, and ethical aspects of the data and are therefore the key individuals responsible for all aspects of the data. In practice, PIs often act as Data Custodian and Data Controller with the respective rights and responsibilities described in later Policy Recommendations sections.</p> <p>The PI is responsible for the integrity of the research that is undertaken, including the ethical compliance component of any collected data. Furthermore, they are responsible for the appropriate treatment of research data. This includes the responsibility for ethical conduct during research leading to data, as well as a choice of appropriate later uses. They are further responsible for ensuring that researchers they employ follow the same ethical code of conduct.</p> <p>Data that were collected outside of the HBP needs the sponsorship of an HBP PI to be integrated into the HBP data flows. In all cases, an HBP PI must accept responsibility for the acceptability of the data.</p>
<a href="#">Processing</a>	Any operation or set of operations which is performed on personal data including data storage, anonymisation, data transfer, etc.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

## 2. Classification of Data and Resulting Requirements

HBP researchers produce and use data from a range of organismal backgrounds and in different contexts. The combinations of different types, origins, and users lead to a variety of requirements for how the data are to be treated.

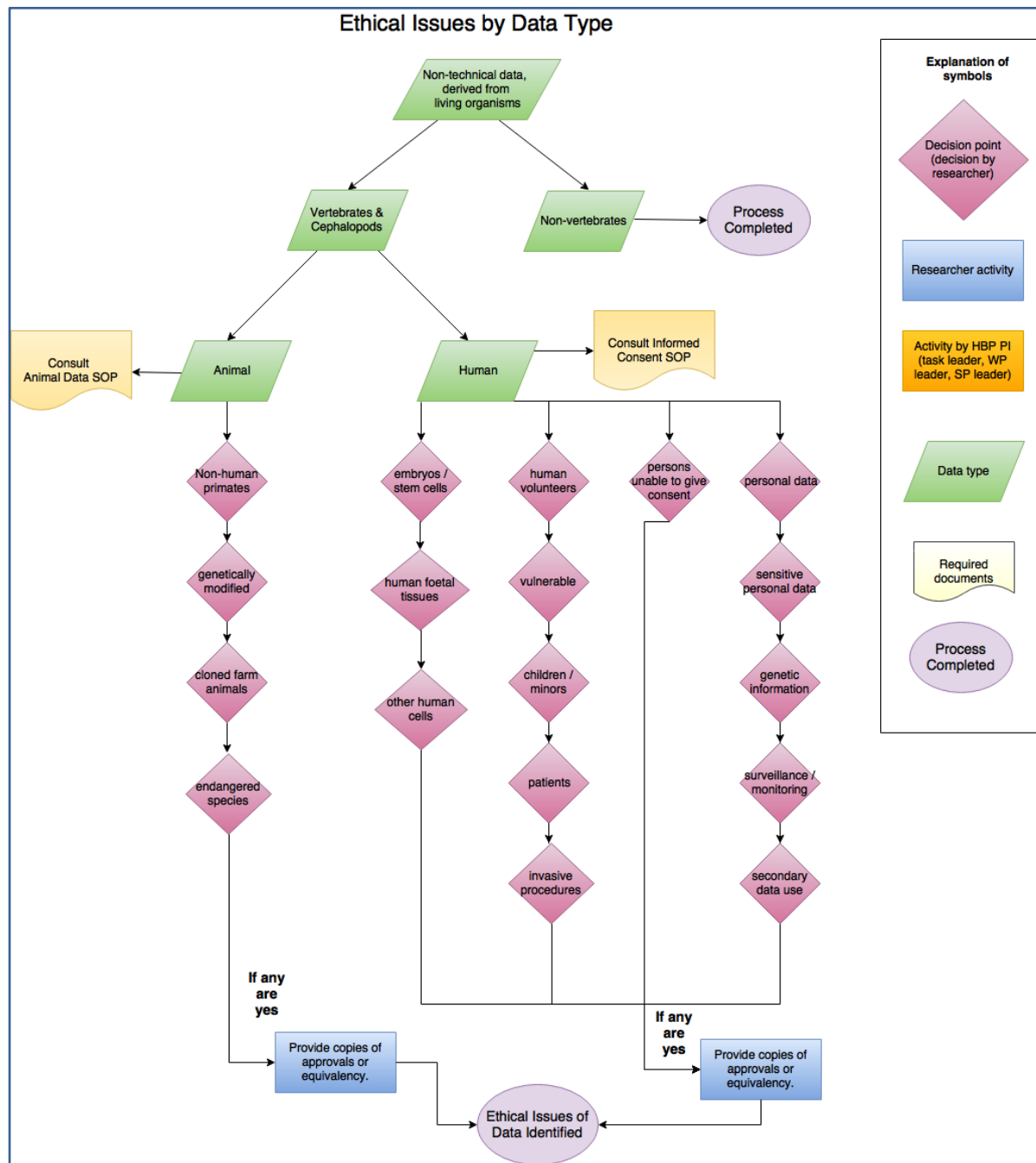
### 2.1 Types of Data

The HBP employs a multi-category typing schema for data which allows filtering (of data) based on source organism, producer, generation/processing steps, and licensing constraints. The typing/classification of data happens for the most part during the initial registration process. Data processed in the HBP digital research infrastructure will retain a record that will allow newly generated data to inherit information based on processing method and source data if available.

### 2.2 Ethical Requirements Based on Source Organism

All data hosted in the HBP digital research infrastructure must be generated in accordance with the ethical and legal principles of the EU and Member States. Key to these is the origin of the data (see also the [Non-EU Animal Data](#) SOP). The following figure describes which ethical issues need to be considered for data that is collected from organisms. Research on organisms (including

humans) normally requires a prior ethics review resulting in an ethics approval. Such an approval, provided by a competent national authority and acceptable in a European Member State is a requirement for the subsequent use of the data in the HBP. While all ethical protocols are controlled for their conformity to national and EU principles, in some cases, the local ethical committee (i.e. that of the institution in which the research is carried out) is made fully responsible for the approved version of the protocols through a “silent consent” mechanism (no adverse comments within 30 days from submission to the national ethical committee). In this case, the code of the ethical protocol is that given by the local (rather than national) ethical committee. The figure shows which aspects should be considered in the ethics approval.



## Part I

### 3. Data Protection Guidance and Policy in the HBP

This section of the DPM focuses on human data with a primary emphasis on application of EU data protection law in the HBP. The point of departure is to provide a standard-setting document for the HBP for applying the General Data Protection Regulation (GDPR) requirements applicable to data handling in the project.<sup>1</sup> In addition to legal requirements and routines, the DPM also contains data inventory worksheets to help identify and collect information regarding data processing activities across the HBP. This information is necessary for addressing the application of the GDPR, confirming the legality of data processing, assessing data protection risks, applying exceptions for [scientific research](#), and gathering information for [Data Protection Impact Assessments \(DPIAs\)](#).

In addition to the GDPR, the DPM also takes account of guidance provided by the European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), and decisions of the Court of Justice for the European Union.<sup>2</sup> Further, the DPM incorporates guidance from national data protection authorities (DPAs) including the CNIL in France, the Information Commissioner's Office (ico) in the UK, Datatilsynet in Norway, and guidance from the European Data Protection Supervisor. The DPM also considers and applies research from the legal academic sources.

The DPM will be updated to reflect EDPB opinions, guidance, and judicial decisions on an ongoing basis. To remain accessible, this version of the DPM attempts to minimise legal analysis and footnotes are kept to a minimum. In some areas such as consent, opinions that are more expansive will also be made available.

#### 3.1 Application, terminology and Icons

The HBP is a large-scale research project employing over 500 scientists at more than 100 universities and research institutes located across Europe and abroad (e.g. Israel, Canada, and the USA). As such an extensive project, the HBP contains a wide range of personal data ranging from Human Resources data to special category data including medical records and genetic data. In short, the HBP's data footprint is massive, complex, and spread globally.



At least one challenge from a data protection perspective is the organisation of the HBP. At the 'HBP layer', the project has infrastructure including a website, decision-making bodies such as the Stakeholder Board (SB), the Steering Committee of the Stakeholder Board (SCSB), and the Directorate (DIR) in addition to dedicated scientific leadership.

In addition to project management at the HBP layer, there are 12 Subprojects where research is primarily conducted and the HBP ICT-platforms are developed. These subprojects are generally comprised of multiple universities or institutions. In many cases, the partners within an SP are located in several countries. For instance, examining SP5 and SP8 we have at least the following institutions in the following countries:

---

<sup>1</sup> 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 (General Data Protection Regulation) henceforth "GDPR." Available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>>.













<sup>2</sup> The EDPB includes representatives from the data protection authorities of each EU member state. The EDPB adopts guidelines GDPR compliance and has endorsed several earlier guidelines/opinions of the WP29. A list of endorsed opinions is available here <[https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb\\_en](https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en)>

 <p>CHUV (Switzerland) EPFL (Switzerland) Tel Aviv U. (Israel) Cardiff U. (UK) AUEB (Greece)</p>	 <p>Oslo University (Norway) Karolinska Institute (Sweden) EPFL (Switzerland) Research Centre Jülich (Germany) Heidelberg Collaboratory for Image Processing (Germany)</p>
---	---



The DPM operates primarily at the ‘HBP layer’ and the ‘SP layer’, and does not broadly consider the legal obligations of the individual partners. Although it is relevant for universities and institutions, the DPM does not provide specific guidance at the institutional level. That is, the DPM does not provide all legal requirements that a hospital in Switzerland or biobank in Germany must follow to achieve GDPR compliance. Universities and institutes at that level must apply and adapt the DPM within their specific regulatory context.

When referring to ‘SPs’ or ‘HBP partners’, the DPM is generally referencing all 12 Subprojects (SPs), all six CoDesign projects (CDPs), all Partnering Projects (PPs), and outside partners when applicable. This acknowledges that each of the SPs (or CDPs) consist of multiple institutions, each with their own data protection obligations.


In many areas of the DPM, the GDPR will be applicable to all actors taking part in the HBP. The following text box and icons indicate project wide application:

Brief description of the requirement
           

If the DPM has special relevance to an SP, a text box will be used followed by an explanation:

	Determination or information relevant to SP1
	Determination or information relevant to SP2

Areas where a derogation for [scientific research](#) is possible will include the following icon and a brief explanation of how the exception or allowance applies. Such exceptions will depend on the laws of the [member state](#).

	Denotes a derogation or allowance relevant to scientific research per GDPR Art. 89.
---	---

General references to HBP Platforms include all six of the primary ICT-based platforms. These are collectively referenced as ‘HBP Platforms’ or ‘HBP infrastructure.’ Additionally, data protection law is applicable to the use of cloud computing services by HBP partners. A separate cloud computing policy has been drafted and is under review by the Data Governance Working Group (DGWG). This policy will be added to the DPM when finalised.



This icon represents areas where the [HBP Data Protection Officer \(DPO\)](#) has additional guidance.

## 3.2 Data Protection Law in the EU

In the EU, the related concepts of privacy and data protection and are granted high legal standing.<sup>3</sup> Although the rights to privacy and data protection are qualified and balanced against other rights and interests, including those of national security and public safety, they nevertheless are weighted heavily.<sup>4</sup>

Since the HBP project began in 2013, EU data protection law has undergone significant changes. In particular, the longstanding Data Protection Directive<sup>5</sup> was replaced by the General Data Protection Regulation (GDPR), which entered into force in 2016 and was applied from 25 May 2018. The GDPR is designed to harmonise EU data protection law and to apply directly and uniformly across all EU member states. Although the GDPR allows for derogations—some of which are directly applicable to the HBP—the overall result is greater harmonisation of data protection law across the EU. While the move from the Directive to the GDPR is important for the HBP, the GDPR does not completely break from the moorings set out in the Directive. Therefore, SPs that were compliant with the Directive will only need to make minimal changes to comply with the GDPR. However, SPs that were not compliant with the Directive have substantial ground to cover in order to meet their compliance burden under the GDPR.

## 3.3 Risk-Based and Scalable Approach to the GDPR

Like the Directive, the GDPR remains a principle-based legislative instrument and requires interpretation. Applying the GDPR to the HBP is an ongoing process. Furthermore, the GDPR takes a ‘risk-based approach’, and obligations are scalable. Therefore, what is required will depend to some extent on the processing activities, the data controller, the type of data, and the overall risks to the data subject. In many instances, application of the GDPR will require a case-by-case assessment. For example, it is not possible to provide one [data retention](#) schedule for the entire HBP. Deletion of data will depend on the [legal basis](#) and the [purposes of processing](#), among other factors. Similarly, [security requirements](#) for processing special categories or [sensitive](#) personal data will be more exacting than requirements for [personal data](#).

## 3.4 Material Scope and Application of European Data Protection Law: Processing of Personal Data

In determining whether activities fall within the material scope of the GDPR, two elements must be evaluated.

<sup>3</sup> See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. See also Article 8 of the European Convention on Human Rights.

<sup>4</sup> GDPR Art 2(2). See also GDPR Recital 4.

<sup>5</sup> 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 (henceforth ‘the Directive’).

First, the data must be ‘*processed*’.<sup>6</sup> The processing of personal data includes “...any operation or set of operations which is performed on personal data...”.<sup>7</sup> Data protection law takes a much broader view of processing than is generally used by technologists and even storage of data is considered processing.

Based on the broad definition, effectively all ICT platforms used in the HBP will meet the definition of ‘processing’ for GDPR purposes. In addition to storage, the process of anonymising data is also considered processing.

There has been some confusion in SPs regarding when processing occurs. For example, some partners have wrongfully assumed that the GDPR does not apply to ‘raw data’ or ‘survey data’ until it is entered into a spreadsheet or database. This position is incorrect. As a rule of thumb, any storage or use of data will be considered processing.



Second, the data must be ‘*personal*’.<sup>8</sup> The intention of focusing on personal data is to protect the rights of the “data subject.” That is, the “identified or identifiable natural person” (data subject) to which the data being processed and collected refers.<sup>9</sup> This protection is limited to natural living persons and thus does not include legal or deceased persons.

An additional category falling outside of the scope of GDPR application is anonymised data. If data are anonymised, they are no longer considered personal.<sup>10</sup> However, given the difficulty in creating truly anonymous datasets, the bar for anonymisation has been set extremely high. Therefore, effectively using this exception in practice is difficult. With certain types of data, such as genetic information, it is unlikely that the data can ever be made anonymous.

### 3.4.1 Personal data in the HBP

**‘General Personal Data’ in the HBP:** Names, telephone numbers, email addresses, identification numbers, account related data such as Human Resources data, location data, IP addresses.

**‘Research Related Personal Data’ in the HBP:** Data concerning health, medical records, genetic data, biometric data, survey data and the results of questionnaires.<sup>11</sup>

**Data NOT Regulated by GDPR in the HBP:**

- 1) animal data,
- 2) data from legal persons such as corporations,
- 3) data of deceased persons,
- 4) anonymised data,
- 5) The GDPR contains additional exceptions for “purely personal or household activity.” However, these exceptions will have little if any application in the HBP.

Even if data fall into a category outside of the GDPR, it is important to evaluate the data broadly. Although the data at issue may not be personal, related data might be personal. For example,

<sup>6</sup> GDPR Art 2(1). Applies to “the processing of personal data”. GDPR Art 4(2). See Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015], [37].

<sup>7</sup> *ibid.* See *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzalez* [2014], [28]. Examples of data processing in the search engine context.

<sup>8</sup> GDPR Art 2(1).

<sup>9</sup> GDPR Art 4(1).

<sup>10</sup> GDPR Recital 26.







<sup>11</sup> GDPR Art 4 (13-15). Defining ‘genetic data’, ‘biometric data’, and ‘data concerning health.’ See further GDPR Art 9.









although data regarding animals are not personal data, records of researchers submitting ethics authorisations are personal data when the authorisations include names, email addresses, or even an ID number that can be used to identify a researcher.

If it becomes possible to de-anonymise data, the data will become personal and the GDPR is applicable.

Therefore, SPs must take a risk-based approach to re-identification. This requires considering what is possible today in addition to what means might be used in the future to re-identify an individual. For example, consider the impact of big data analytics. Many of the tools and insights under development in the HBP are exactly the type of tools that might be used to make re-identification possible.


 <b>SP1</b>	<ol style="list-style-type: none"> <li>1) Animal data—GDPR is not applicable.</li> <li>2) Records of researchers submitting ethics authorisations—GDPR is applicable when that data are personal</li> <li>3) ‘General Personal Data’ as defined above—GDPR is applicable</li> </ol>
 <b>SP2</b>	<ol style="list-style-type: none"> <li>1) ‘Research Related Personal Data’ as defined above —GDPR is applicable</li> <li>2) Sensitive Personal Data—GDPR is applicable</li> <li>3) ‘General Personal Data’ as defined above—GDPR is applicable</li> <li>4) Anonymised data—GDPR not applicable, but see risks related to anonymisation above.</li> </ol>
 <b>SP3</b>	<ol style="list-style-type: none"> <li>1) Animal data—GDPR is not applicable.</li> <li>2) Records of researchers submitting ethics authorisations—GDPR is applicable when data are personal</li> <li>3) ‘Research Related Personal Data’ as defined above —GDPR is applicable</li> <li>4) Sensitive Personal Data—GDPR is applicable.</li> <li>5) ‘General Personal Data’ as defined above—GDPR is applicable</li> <li>6) Anonymised data—GDPR not applicable, but see risks related to anonymisation.</li> </ol>
 <b>SP4</b>	<ol style="list-style-type: none"> <li>1) ‘Research Related Personal Data’ as defined above —GDPR is applicable</li> <li>2) ‘General Personal Data’ as defined above—GDPR is applicable</li> </ol>
 <b>SP5</b>	<ol style="list-style-type: none"> <li>1) Animal data—GDPR is <b>not</b> applicable.</li> <li>2) Data of deceased persons (e.g. ex vivo data)—GDPR is <b>not</b> applicable.</li> <li>3) Records of researchers submitting ethics authorisations—GDPR is applicable when data are personal</li> <li>4) ‘General Personal Data’ as defined above—GDPR is applicable</li> <li>5) Anonymised data—GDPR not applicable, but see risks related to anonymisation.</li> </ol>
 <b>SP6</b>	<ol style="list-style-type: none"> <li>1) Animal data—GDPR is <b>not</b> applicable.</li> <li>2) Records of researchers submitting ethics authorisations—GDPR is applicable when data are personal</li> <li>3) ‘Research Related Personal Data’ as defined above —GDPR is applicable</li> <li>4) ‘General HBP data’ as defined above—GDPR is applicable</li> </ol>



	1) 'General HBP data' as defined above—GDPR is applicable. In particular, user account information.
	1) Records of researchers submitting ethics authorisations—GDPR is applicable when data are personal 2) 'Research Related Personal Data' as defined above —GDPR is applicable 3) Sensitive Personal Data—GDPR is applicable (e.g. patient records on the MIP local). 4) 'General Personal Data' as defined above—GDPR is applicable 5) Anonymised data—GDPR not applicable, but see risks related to anonymisation.
	1) 'Research Related Personal Data' as defined above —GDPR is applicable 2) Sensitive Personal Data—GDPR is applicable (e.g. biometric/voice data 3) 'General Personal Data' as defined above—GDPR is applicable
	1) 'General HBP data' as defined above—GDPR is applicable. In particular, user account information.
	1) 'General HBP data' as defined above—GDPR is applicable. In particular, user account information.
	1) 'General HBP data' as defined above—GDPR is applicable. In particular, user account information. This also includes personal data collected to ethics submissions. 2) 'Research Related Personal Data' as defined above —GDPR is applicable. In particular, survey data and the results of questionnaires depending on subject matter.

### 3.4.2 Special categories ('sensitive') personal data



















The GDPR provides that the processing of personal data “revealing racial or ethnic origin...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 shall be prohibited.”<sup>12</sup> In some instances, minutes of HBP governing bodies might also be considered sensitive personal data. In particular, where such minutes reveal personal data related to racial or ethnic origin, political opinions, or other categories of sensitive personal data.

	<b>Possible Scientific Allowance:</b> <a href="#">GDPR Art 9(2) (j)</a> providing a legal basis for processing special categories of data in some circumstances. <sup>13</sup> <b>Possible additional Limits:</b> GDPR Art 9(4) allowing member states to introduce further conditions, including limits, regarding the processing of genetic data, biometric data or data concerning health.
---	--


There are exceptions to the prohibition (i.e. explicit consent) that are evaluated further in the [legal basis](#) section below.

<sup>12</sup> GDPR Art 9.

<sup>13</sup> To apply GDPR Art 9(2)(j) you must also have a legal basis under GDPR Art 6 (e.g. 6(1) (e or f)).

	No sensitive personal data
	Genetic data/ data concerning health
	data concerning health
	Data concerning health
	Biometric data (voice identification)
	Survey data and the results of questionnaires may concern health
<p>SPs are responsible for processing all personal data in a GDPR compliant manner. If data does not fall into a clearly excluded category under the GDPR (e.g. animal data, data from deceased persons) then the SP must comply with the GDPR.</p> <p>When relying on anonymisation, SPs must take a broad approach in their determination and consider 'all the means reasonably likely to be used' to identify the individual.</p> <p>The GDPR applies broadly and is <u>not limited</u> to medical records and genetic data. Contact details such as email information and IP addresses are also personal data.</p>	
           	

The inventory below is a tool of SPs to evaluate the data they have in their project as personal.

 <h2>Human Brain Project</h2>
<b>Data Processing Inventory: Data Types (Personal Data and non-Personal data)</b> Fill in the following categories. For further explanation, see the DPM.
<ol style="list-style-type: none"> <li>Does the subproject, research, or administrative activity process personal data? This includes: names, telephone numbers, email addresses, identification numbers, account related data such as human resources data and billing information, location data, IP addresses.</li> <li>Does the subproject or research activity process sensitive personal data? This includes: Data concerning health, medical records, genetic data, biometric data, and in some instances, survey data and the results of questionnaires.</li> </ol> <p>If the Answer to (1) or (2) is yes, the GDPR is applicable. If you answered yes to (2), the data are 'special category data' and processing will require an additional legal basis (GDPR Article 9).</p>

If the subproject, research, or administrative activity concerns: animal data, data from legal persons, data of deceased persons, or anonymised data the GDPR is not applicable. However, SPs must consider the following:

- 3) Are personal data being collected in conjunction with the non-personal research data? For example, do the animal data also contain the names or identification numbers that can be linked back to researchers?

If the Answer to (3) is yes, the GDPR will apply to ‘related’ personal data.

If [anonymised data](#) become de-anonymised, they will be considered personal and the GDPR will apply.

### 3.4.3 Territorial Application of the GDPR to the HBP

The GDPR applies to [data controllers](#) and [data processors](#) established in the EU. All HBP partners located in the EU are subject to the GDPR.

- 1) If data are transferred from outside of the EU to an HBP partner located in the EU, and the HBP partner processes that data, the GDPR is applicable to these data. For example, if a Chinese partner transfers data to SP5, and HBP partners process these data, the GDPR will apply to the data of the Chinese partner. The result is that it may be difficult to transfer these data back to the Chinese partner (see [data transfers](#)).
- 2) The GDPR is also applicable to data controllers or processors offering goods or services in the EU or monitoring the behaviour of individuals in the EU.

All HBP partners located in the EU are subject to the GDPR.



## 3.5 Data Processors and Data Controllers: Roles and Responsibilities

The GDPR assigns data processing obligations and responsibilities based largely on whether a party is a data ‘processor’ or a data ‘controller’.<sup>14</sup> The controller/processor relationship largely boils down to an allocation of responsibility. Understanding these concepts and their interactions is essential to applying the GDPR to the HBP.<sup>15</sup> The roles are defined in the GDPR as:

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means* of the processing of personal data...;

‘processor’ means a natural or legal person, public authority, agency or other body which *processes personal data on behalf of the controller*...<sup>16</sup>

Under the GDPR, data controllers have the primary responsibility for treating the personal data entrusted to them in conformance with the law. The primary component necessary to meet the controller designation is that the natural or legal person makes a specific determination regarding

<sup>14</sup> GDPR Art 4 (7) & (8), respectively.

<sup>15</sup> WP29 ‘Opinion 169 1/2010 on the concepts of “controller” and “processor”’ (2010) 1-35, 2. (henceforth ‘WP29 169’).

<sup>16</sup> GDPR Art 4 (7) & (8) emphasis added. See also GDPR Art 24 and 28.

“the purposes and means” of data processing. Specifically, does the actor determine the ‘how’ and the ‘why’ of data processing?

The GDPR also provides for “joint” controllership if responsibility is shared.<sup>17</sup> This is relevant for SPs that share and process personal data within their research areas. Joint controllers have some flexibility in allocating obligations and responsibilities, as long a full compliance is obtained.<sup>18</sup>

### 3.5.1 Data Controllers in the HBP

**Organisation:** The role of the HBP as a ‘data controller’ or a ‘joint controller’ prior to obtaining Legal Entity (LE) status remains an area of ongoing discussion. The HBP DPO is of the opinion that the HBP cannot avoid all data controller or joint data controller liability under the GDPR. This is likely the case even if it does not have a traditional legal form. There are several key areas where the HBP will likely be deemed a data controller or joint controller where the HBP determines ‘the purposes and means of data processing. In particular, the complexity of the project and the wide range of data sharing it facilitates creates a complex and unclear picture for data subjects regarding the processing of their data. In many areas, the HBP provides instructions to SPs and heavily influences the purposes and means of data processing. In these areas, the DPO is of the opinion that the HBP will likely be considered a data controller or a joint controller.

Following a final determination or transition to an LE, adjustments to the DPM will be required. Until that point, it assumed that the institution/hospital/university would be deemed data controllers and that the HBP is not a joint controller.



A more expansive legal analysis of this issue is available in a memorandum on file with the DPO.

As a project, the HBP is currently following a modified “origin-based” approach to controllership. This approach obliges the SP institution/hospital/university to comply with the GDPR as required by their institution/hospital/university and the laws of their member state. When submitting data to HBP Platforms, such as the SP5 NIP or the SP8 MIP, partners are required to certify that the data they are providing is in compliance with the GDPR along with all other ethical compliance requirements.

In most cases, data subjects will contact the hospital or institution to ask questions, exercise [individual rights](#), or withdraw consent. However, platform providers—and the HBP partners generally—must also assist data subjects in addressing questions, complaints, or concerns regarding data processing in the project.

**General categorisations:** Determining controllership requires a specific analysis of the data processing that takes place. However, some general classifications are applicable to the HBP:

- Institutions/universities/hospitals collecting and processing personal data will be data controllers and are responsible for compliance.
- As platform operators HBP partners will generally be considered controllers or joint controllers, depending on their actions and data processing operations.
- Cloud service providers and IT-hosting providers will be considered data processors.

All HBP partners will have some data controller liability. Whether the personal data is contact information, location data, or sensitive personal data, the SP or partner is required to meet legal requirements. General guidelines that HBP partners can generally apply with SPs are:

<sup>17</sup> GDPR Art 26.

<sup>18</sup> GDPR Art 26 (1). See also WP29 169 (2010) 24.

- 1) The SP partner collecting names and email addresses for a conference/webinar will be a data controller regarding that information.
- 2) The SP partner collecting human resources data personal data such as account numbers, names and email addresses of employees, and other personal data necessary to administer the project will be a data controller.
- 3) The local hospital or institution that collects personal data and has access/control over data will be the data controller for that information. This includes sensitive data such as human data, medical records, and biometric data.
- 4) Researchers using surveys will be responsible for personal data collected as part of that research.
- 5) In many cases, individual institutions provide data that they will share for research purposes with other SP partners. If two or more controllers jointly determine “the purposes and means of processing”, they may be considered joint controllers. The partners will have responsibility for their individual processing.





### 3.5.2 Data processors in the HBP

To qualify as a processor, two conditions must be met. First, the party must be a separate legal entity from the controller. Second, the processor must process data “only on documented instructions from the controller.”<sup>19</sup>

Being deemed a data processor has several advantages including a favourable apportionment of liability. However, the practice of attempting to designate the ‘controller’ and ‘processor’ roles in contract terms (e.g. ToUs/ToS) will not negate responsibility under the GDPR. That is, contracts providing that a partner or even the HBP will always be deemed a processor are ineffective and do not negate the requirements set out by the GDPR.

The GDPR places requirements on parties based on their actual roles or conduct in data processing operations and not simply on the labels they give themselves. Therefore, looking at what the parties actually do, rather than how they define their roles contractually, is dispositive when applying the GDPR. Processors now have direct responsibilities and obligations under the GDPR and can be held directly responsible for non-compliance with these obligations.

	<p><b>Example:</b> If SP7 partners only provide access to infrastructure, they will be considered data processor for those purposes. If SP7 partners process login data (e.g. researcher credentials), it will be deemed a data controller for those purposes.</p>
<p><b>HBP subclass - Data Repository Service Operator</b></p> <p>In the HBP, this role can be seen as a specific subclass of Data Processor which installs and operates a service used by another Data Controller or Data Producer. While not defined in the GDPR, the Data Repository Service Operator is a common label used in the HBP and it should be clear that this should be considered a GDPR Data Processor.</p>	
	

<sup>19</sup> GDPR Art 28(3)(a).

## 3.6 Data processing agreements and SP Controllers

In most cases, SP controllers must have a data processing contract in place before enlisting a processor.<sup>20</sup> SP controllers may only enlist data processors that provide ‘sufficient guarantees.’

SP partners must include the following *general details* in their contract with data processor:

- the subject matter and duration of the processing,
- the nature and purpose of the processing,
- the type of personal data and categories of data subject, and
- the obligations and rights of the controller.

Specific *contractual obligations* include the following:<sup>21</sup>

- the processor must only act on the written instructions of the controller (HBP partner(s))<sup>22</sup>
- the processor is committed to confidentiality requirements.<sup>23</sup>
- the processor must take appropriate measures to ensure the security of processing<sup>24</sup>;
- the processor may only subcontract (engages a subprocessor) with “prior specific or general written authorisation of the controller”;<sup>25</sup>
- the processor must assist the data controller in allowing data subjects to exercise their rights under the GDPR;
- the processor must also assist the controller in ensuring compliance with GDPR obligations, including security, data breach, and data protection impact assessments (DPIAs);<sup>26</sup>
- the processor deletes or returns all the personal data to the controller after the relationship ends;<sup>27</sup> and:
- the processor makes information available to the controller to assist with audits and inspections.<sup>28</sup>

The contractual requirements contained in GDPR Article 28 are extremely prescriptive.<sup>29</sup> Although the EC has not yet provided a standard data processing contract, it is likely that standard agreements will eventually be made available. A sample/model agreement is available [here](#).<sup>30</sup>

SPs should note that not all providers offer a data-sharing contract. This is often the case for US-based ‘free’ cloud services. The HBP cloud computing policy evaluates this issue and will be included in the DPM inventories and worksheets when it is approved.

---

<sup>20</sup> GDPR Art 28(3).

<sup>21</sup> Requirements are based on GDPR Art 28(3) (a-c).

<sup>22</sup> GDPR Art 28(3)(a).

<sup>23</sup> GDPR Art 28(3)(b).

<sup>24</sup> GDPR Art 28(3)(c). Including security measures as required per GDPR Art 32.

<sup>25</sup> GDPR Art 28(2).

<sup>26</sup> GDPR Art 28(3)(f).

<sup>27</sup> GDPR Art 28(3)(g). This end of contract requirement applies “... unless Union or Member State law requires storage of the personal data.”

<sup>28</sup> GDPR Art 28(3)(h).

<sup>29</sup> GDPR Art 28(5).

<sup>30</sup> <https://www.dlapiper.com/en/us/insights/publications/2017/08/example-gdpr-ready-processor-terms/>



## 3.7 Principles Relating to Data Quality and Application to the HBP

As adopted, the GDPR principles relating to the processing of personal data closely follow the approach taken in the Directive. These principles make up the core of data protection law in the EU and must be incorporated into the HBP as a whole and accounted for throughout the SPs. The following part describes the principles generally and then provides examples of how they might be accounted for in the HBP.



### 3.7.1 *Data must be processed fairly, lawfully, and transparently*

Of particular import is the principle that data must be “processed lawfully, fairly and in a transparent manner...”.<sup>31</sup> Despite its somewhat vague character, this principle is fundamental to data protection and is applicable to all other principles described in this section.

**Lawfully:** for processing to be ‘lawful’, the controller must have a specific and appropriate [legal basis](#) for the data processing for the entire period of processing. This also includes following general legal requirements such as confidentiality requirements and contract terms.

SPs must have a legal basis for processing of personal data (e.g. performance of a contract, legal obligation, and legitimate interest, among others). Although these are expanded upon in the next section, for much of the research conducted in the HBP the legal basis is consent. Depending on the data processed by the SP partners, legal requirements will also vary. For example, many member states have confidentiality requirements for medical records or medical data independent of the GDPR. A breach of such confidentiality requirements also amounts to a breach of the lawfulness principle.

**Fairly:** In addition to having an appropriate legal basis for processing, the HBP SP partners must also process data fairly. 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.

For example, failing to provide the data subject with adequate information regarding the technology used in the processing, thus reducing their ability to control and make decisions about the processing, is likely unfair. Repurposing, selling, or reusing data in a manner that goes beyond the consent provided by the data subject is clearly unfair. Furthermore, failure to provide adequate or complete information, or to otherwise process data in a manner inconsistent with a privacy policy or contract is also unfair.

**Transparency:** As a key concept running throughout the GDPR, the element of ‘transparency’ is essential to the fair and legitimate processing of data. At the concept’s core is the notion that the data subject must be provided with adequate and accurate information regarding processing activities.

<sup>31</sup> GDPR Art 5(1)(a).



## Transparency in the HBP

SP partners should maintain and provide data subjects (e.g. research participants) with clear information about:

- 1) The identity of the controller (e.g. name of hospital/institution and contact information). If there are multiple controllers, or joint controllers, this information should also be provided.
- 2) The legal basis for processing. If the legal basis is consent, the data subject should be informed on the procedure for withdrawing consent.
- 3) The purposes of the processing (e.g. medical research). This should be made as clear as possible, particularly if the data might be processed in ways the data subject might not expect.
- 4) The extent of processing. If the data will be processed by users outside of the hospital/institution or made accessible to third parties, the data subject must be informed. Even if the data will be anonymised before it is shared, the data subject must be made aware of that process so they might assess the associated risks.
- 5) Provide information on how data subjects can exercise their rights (rectification, erasure etc.). In particular, provide data subjects with contact information for their Data Protection Officer ([DPO](#)).

The above information must be provided to the data subject in a clear and accessible manner, for example, as part of the informed consent. The HBP website should also provide this information.



### 3.7.2 Purpose specification and limitation principle

The GDPR requires that data be collected for “...specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes...”.<sup>32</sup> Compliance requires that a sufficiently narrow purpose for data processing must be set prior to the collection of personal data. Data collection must not exceed what is necessary to fulfil that purpose.

Any further use of the data must be compatible with the original purpose. Central factors for this evaluation include the relationship between the purposes, context and reasonable expectation of the data subject, nature of the data, and safeguards.

If data are processed in a manner that is incompatible with the purpose for which it was initially obtained, the processing is unlawful.<sup>33</sup> If data are used for a purpose beyond that for which it was collected, it is considered to have been ‘repurposed’. Repurposing data might include acts such as selling personal information for advertising purposes or other acts beyond the consent provided by the data subject.<sup>34</sup>

All SP partners must set a purpose for data processing and limit processing to that purpose

- Clearly identify the purpose for the data processing (e.g. scientific research, completion of a contract, dissemination) before processing begins.

<sup>32</sup> GDPR Art 5(1)(b) and GDPR Recital 39.

<sup>33</sup> GDPR Art 6(4). An incompatible purpose (i.e. ‘repurposed’) data cannot be later legitimised by changing to a new legal basis. WP29 203 (2013) 36.

<sup>34</sup> GDPR Art 89.

- Limit the amount of data collected to what is necessary to fulfil the purpose.
- Communicate the purpose of processing to data subjects.
- Inform data subject to any changes to the primary purpose of data processing.
- If further processing will take place, provide a written determination of whether the new purpose is compatible.



**Scientific Allowance:** Research conducted for scientific purposes will not be considered incompatible with the initial purposes, if the requirements of GDPR Article 89 (1) have been met. These requirements are evaluated further in the [Scientific Research](#) Section. In short, if available in the SP partners member state, this is an important exception for research.

### 3.7.3 Data minimisation

In addition to attaching a specific purpose to data collection, the principle of data minimisation requires that data collected be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”<sup>35</sup> What is necessary or relevant will depend on the purpose of the data collection. Simply stated, this principle requires that controllers limit the amount of data they collect to what is necessary to fulfil the [purpose](#) set for data processing.

In addition to collecting less data, once the purpose has been fulfilled, data should be deleted or anonymised. This principle is particularly important for data protection by [design and by default](#).

#### 3.7.3.1 Data minimisation in the HBP

All SPs must implement data minimisation. This is an important aspect of the exceptions provided for [scientific research](#).

- SPs must limit their data collection to that which is directly relevant from the specified purposes.
- Whenever possible, use anonymisation and pseudonymisation techniques.



### 3.7.4 Data accuracy and quality

Data must also be “accurate and, where necessary, kept up to date.”<sup>36</sup> If data are not accurate, the data must be erased or corrected. If the data are inaccurate, the data subject has a right to have the data rectified or even object to the processing of data concerning them.

<sup>35</sup> GDPR Art 5(c).

<sup>36</sup> GDPR Art 5(d).

### 3.7.4.1 Data Accuracy and Quality in the HBP

All SP partners must implement data quality and accuracy controls.

- Ensure that records are accurate and kept up to data
- Develop procedures to maintain accuracy through updates, system audits, and other procedures to check that information is accurate.
- Provide data subjects with the means to rectify data if they are no longer accurate. For example, on a webpage providing information on the purposes of research also provide contact information for data subjects.



### 3.7.5 Storage limitation and deletion:

Once the purpose of data collection has been completed, the general rule is that data should be erased or deleted.<sup>37</sup> Retention periods will vary depending on the purpose of the initial collection. However, the duty applies whether the data are stored on a local hard drive or a global server farm with worldwide infrastructure.

If other legal regulations limit the ability of the controller to erase the data, including bookkeeping or audit requirements, the data can be stored for longer periods. In that case, the data must be secured appropriately and erased when it becomes legally possible. This may generally be accomplished by destroying the medium or through sufficient overwriting.<sup>38</sup> The GDPR specifies that deletion requirements should be contained in the controller/processor contract.<sup>39</sup>

#### 3.7.5.1 Storage limitation and deletion in the HBP



All SP partners must evaluate data storage limitation/data retention

- Assess retention time needed to fulfil the purpose. If the purpose of the data processing is completed, what is your legal basis for retaining the data? If the data are no longer needed, it should be securely deleted.
- There is no 'one size fits all' period. In some cases, data will only be necessary for the life of the project (e.g. contact information). Other data, such data committed to the MIP or NIP will be stored for much longer periods as is necessary for research.
- Partners may be required to keep accounting data for much longer periods than the life of the project for audit purposes. This is allowed under the GDPR, but requires a legal basis. Generally, a specific bookkeeping law or accounting requirement will be sufficient.
- When SP partners design systems, they should track and differentiate data storage for different purposes. They should also have in place procedures for anonymisation and deletion of data once data retention periods end.

<sup>37</sup> GDPR Art 5(e). For purposes in the public interest, including archives, personal data may be stored for longer periods pursuant to GDPR Art 89(1).

<sup>38</sup> WP29 196 (2012) 12. This requires that all copies of the data, including temporary files and file fragments, be erased irretrievably

<sup>39</sup> GDPR Art 28(3)(g).

											
		<b>Scientific Allowance:</b> Research conducted for scientific purposes can be kept for longer periods. This requires meeting the requirements of Art. 89 (1) (see <a href="#">Scientific Research</a> Section) and applying appropriate organisational and technical measures.									

### 3.7.6 Integrity and Confidentiality


Parties with access to personal data must exercise confidentiality in processing or handling such data “...in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage...”<sup>40</sup>.

Meeting the ‘security principle’ requires that SP partners have adequate organisational policies, undergo risk assessments, and put in place technical measures to protect and ensure availability of personal data. The term ‘security’ should be broadly construed and include the protection of networks and information systems on a physical and logical basis. Further, in addition to applying adequate security practices, data controllers should maintain adequate backup. Among other aspects, this requires that controllers choose processors that also offer adequate security and organisational measures.

The GDPR does not provide one security requirement that will apply across the HBP. Security requirements are scalable and they will vary depending on data processing operations, the state of the art, cost of implementation, the overall risk, among other factors provided in GDPR Article 32.

Although compliance requirements are not specifically prescribed, adopting certification schemes and meeting industry standards are a recognised means of meeting this requirement. In many cases, it will be appropriate to apply encryption and/or pseudonymisation techniques to meet this principle.

In addition to putting adequate security in place, this also requires the means to test the effectiveness of such measures. This is not a one-off procedure, and a review process and the means to make improvements in security practices are necessary.

SP partners must meet confidentiality, integrity and availability requirements. As a starting point:											
<ul style="list-style-type: none"> <li>• Ensure that all personal data are secure. This includes data stored using cloud services and web-based email services. For further information, see the HBP Cloud Computing Policy.</li> <li>• Before adding a new technology, perform a security risk assessment and determine whether risks can be adequately mitigated. For further information, see the HBP DPIA Policy.</li> <li>• Design and implement adequate organisational and technical measures to meet the risks. If risks cannot adequately addressed, find a new way to implement the technology or discontinue use of the service.</li> </ul>											
											

<sup>40</sup> GDPR Art 5(f).

The following risk assessment can be used for an initial evaluation and as a means document compliance with the HBP. Further measures are provided in the [DPIA section](#).



HBP Risk Assessment						
Risks	Effects on Data subjects	Sources of Risks	Threats	Existing or planned Security measures	Severity if the risk occurs	Likelihood that the risk will occur
Unlawful Access						
Unwanted modification to HBP Data						
Loss of Data						
Loss of Availability						

### 3.7.7 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.<sup>41</sup> Although this principle has existed in practice in some member states and is already an element of data privacy law internationally, it is an addition to the GDPR. To meet this principle, SPs will be required to document their compliance with the above principles.<sup>42</sup>

### 3.7.8 Accountability in the HBP

**SP Controllers** must be able to demonstrate compliance with the above principles. In practice, this means that SP partners must be able to document and provide evidence that they have complied with the principles. In particular, SP partners should:

- Keep a copy of the data processing agreement they have with sub processors including cloud service provider available for audit.
- Show that the SP partners have implemented DGWG policies and met the requirements of the DPM.
- Demonstrate that appropriate security measures are in place. This includes following best practices, including applying relevant codes of conduct and meeting industry standards. If a certification has been met, documenting and maintaining the certification is appropriate.
- Put appropriate data protection measures in place throughout the entire lifecycle of HBP processing operations. This includes documenting that data are secured using encryption or

<sup>41</sup> GDPR Art 5(2).

<sup>42</sup> GDPR Art 24(1).









other techniques. When the purpose for which the data are collected has ceased, document the deletion process.

- Keeping records of all data breaches. When required, reporting such data breaches to the relevant data protection authority is necessary.
- Records of DPIA, PIAs, and other procedures for reducing or limiting the risks to data subjects are essential. If a DPIA or a PIA has been completed, make a redacted copy of the information available for data subjects.
- Review accountability measures on an annual basis.



Although not specifically required by the GDPR, the use of icons are an effective means to communicate data collection practices and compliance with the GDPR.<sup>43</sup> SP partners should also consider using such icons when possible to provide more accessible explanations of how they use personal data. Icons can be used as part of a privacy policy, an informed consent form, or any other place where there is an intention to communicate data protection practices to research subjects or the public.

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are <b>collected</b> beyond the minimum necessary for each specific purpose of the <b>processing</b>	
	No personal data are <b>retained</b> beyond the minimum necessary for each specific purpose of the processing	
	No personal data are <b>processed</b> for purposes other than the purposes for which they were collected	
	No personal data are <b>disseminated</b> to commercial third parties	
	No personal data are <b>sold</b> or <b>rented out</b>	
	No personal data are retained in <b>unencrypted</b> form	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

<sup>43</sup> Esayas S., Mahler T., McGillivray K., 'Is a Picture Worth a Thousand Terms? Visualising Contract Terms and Data Protection Requirements for Cloud Computing Users' (2016) Current Trends in Web Engineering (ICWE) Lecture Notes in Computer Science. Available at <[https://link.springer.com/chapter/10.1007%2F978-3-319-46963-8\\_4#Sec3](https://link.springer.com/chapter/10.1007%2F978-3-319-46963-8_4#Sec3)>.

## 3.8 Legal basis for lawful Processing of Personal Data

The GDPR requires a legal basis for any processing of personal data.<sup>44</sup> For processing to be lawful, the controller must have legitimate grounds for the duration of the processing.<sup>45</sup> The basis for processing must be determined at the beginning of processing, and there is little flexibility for amendment after processing has begun. In the HBP, likely bases for processing activities include the following examples:

- **Consent**<sup>46</sup>: Consent will generally be required for research. In some cases, it will serve as the basis used for research on personal (see [consent requirements for scientific research](#)). However, consent will not always be the most appropriate legal basis and in some cases will not provide a lawful basis under the GDPR. For example, in employment situations consent will generally be invalid. Additionally, consent can be withdrawn. Therefore, SPs should consider whether one of the categories below interest might provide a more flexible and appropriate basis to support research. For public providers and universities, this will often be
- **Performance of a contract**<sup>47</sup>: If the SP partners have to complete a reimbursement and requires bank account/contact information, they have a clear legal basis to do so under the basis of the performance of a contract. However, once that purpose is completed, the data should generally be deleted in the absence of another legal basis.
- **Legal obligation**<sup>48</sup>: A national law requires that the SP partners retain certain data, such as accounting data, for a specific period. In such a case, the SP partners would be able to store name and account information even after the ‘performance of a contract’ was complete.
- **Vital interests**<sup>49</sup>: If processing becomes necessary to protect someone’s life.
- **Public interest/official authority**: Research organisations that are public authorities may use this basis for conducting research.<sup>50</sup> To use this legal basis, the SP partners must be able to show that it is necessary to process the personal data for its research purpose (i.e. proportionate, reasonable, necessary) and point to a clear legal (supplementary) basis under national law. This is often contained in a university research or national research act (e.g. NHS Act 2006, UK Health and Social Care Act 2012, the the Health Research Act in Norway).

As of November 2018, this is some variance in the guidance among member states on how broadly this legal basis might be used and the level of consent required in secondary data use. Much of the UK guidance suggests consent is required for research, but that data processing for GDPR purposes should rely on public interest/official authority rather than consent.<sup>51</sup> In Norway, guidance suggests that consent will remain central.

- **Legitimate interests**<sup>52</sup>: Provides a flexible basis for processing personal data in way that the data subject might reasonably expect. A determination as to the legitimate interest must take place, and be documented, prior to applying this basis. SP partners relying on this legal basis should provide a written analysis addressing the following (3) elements:

<sup>44</sup> GDPR Art 6(1) (a-f).

<sup>45</sup> GDPR Art 6.

<sup>46</sup> GDPR Art 6(1)(a). Consent is further defined in GDPR Art 4(11). The conditions for lawful consent are provided in GDPR Art 7. See also GDPR Recitals 32, 33, 42, 43.

<sup>47</sup> GDPR Art 6(1)(b).

<sup>48</sup> GDPR Art 6(1)(c) and GDPR Art 6(3). See GDPR Recital 41.

<sup>49</sup> GDPR Art 6(1)(d). This is generally only applicable in matters of life or death (e.g. national disasters). See Recital 46.

<sup>50</sup> GDPR Art 6(1)(e). If sensitive or special category data (i.e. medical research) also GDPR Art 9(2)(j).

<sup>51</sup> Guidance from UK National Working Groups on the GDPR available [here](#).

<sup>52</sup> GDPR Art 6(1)(f). Requires balancing the identified interest against whether the processing is necessary to achieve that interest.



- 1) The processing is necessary to achieve that legitimate interest. For example, ethics reporting.
- 2) Balancing the data processing against the interests of third parties. Would the processing cause unjustified harm or interfere with the individual's interests, rights, or freedom. Can the data subject reasonably expect the processing to take place for this type of activity?
- 3) Are the SP partners collecting the Minimum amount of data necessary to achieve the interest?

Overlap between or among these grounds is possible, and data processing activities may be justified based on one or more of the aforementioned legal grounds. Furthermore, the GDPR largely follows the approach of the Directive. Therefore, SPs will be able to continue using the legal basis they have applied to their processing. However, the GDPR places greater emphasis on accountability and documentation. For commercial research partners, this basis is often applied as the “public interest/official authority” is not available to private providers.<sup>53</sup> Public authorities cannot rely on legitimate interests.

Controllers must be able to demonstrate that they have a legal basis for processing, the basis exists for the entire time of the processing, and that the processing is necessary to complete the purpose. For the processing of sensitive data, including medical data, an additional basis must be provided (e.g. explicit consent).<sup>54</sup> Choosing a basis requires consideration of the processing activities, and then selecting the most appropriate basis.

HBP SP partners must have a legal basis for data processing. This information is required for the entire time data is processed. The ‘data inventory’ below is a tool for determining the legal basis of data processing and accounting for data protection principles.

The data inventory is also helpful for compliance with [documentation](#) requirements.



<sup>53</sup> GDPR Art 6(1)(f). If sensitive or special category data (i.e. medical research) also GDPR Art 9(2)(j).

<sup>54</sup> See GDPR Art. 9.



## Human Brain Project

### Data Processing Inventory Checklist: Principles and Legal Basis

Fill in the following categories. For further explanation, see the DPM.

#### Principles

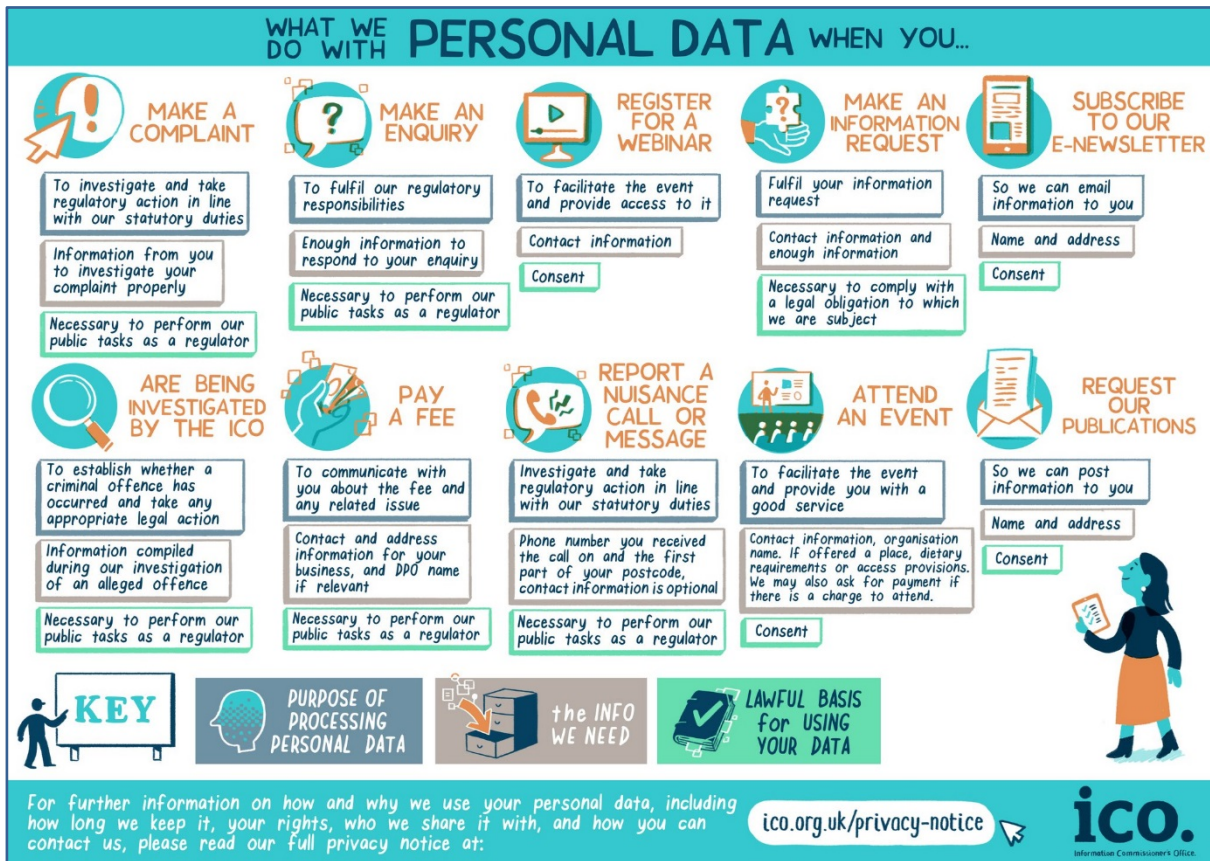
- 1) What is the [purpose](#) of data processing?
  - a) Are the data collected relevant and not excessive for this purpose?
  - b) Are data used for purposes other than as initially collected?
  - c) Are data stored longer than is necessary to achieve this purpose?
  - d) Are data kept secure? Are appropriate technical and organisational measures in place?
  - e) Are data kept accurate and up to date for the purpose?
  - f) Are data transferred to a non-EU/third country.

#### Legal Basis

- 2) What is the [legal basis](#) for data processing (e.g. consent, performance of a contract, legal obligation, etc.)? If more than one basis, explain which basis is used to fulfil each purpose.
  - a) Did the basis exist prior to the start of processing?
  - b) Will this legal basis remain during the entire period of processing?

As a whole, the HBP should consider effective ways of informing participants of how the HBP uses personal data, and the legal basis for data processing. Below is an example from the UK ico that clearly provides (1) the [purpose](#) of processing, (2) the [data necessary](#) for the processing, and (3) the [lawful basis](#):

### 3.8.1 UK ico PrivacyPolicy



**WHAT WE DO WITH PERSONAL DATA WHEN YOU...**

Scenario	Purpose of Processing	Information Needed	Lawful Basis
<b>MAKE A COMPLAINT</b>	To investigate and take regulatory action in line with our statutory duties	Information from you to investigate your complaint properly	Necessary to perform our public tasks as a regulator
<b>MAKE AN ENQUIRY</b>	To fulfil our regulatory responsibilities	Enough information to respond to your enquiry	Necessary to perform our public tasks as a regulator
<b>REGISTER FOR A WEBINAR</b>	To facilitate the event and provide access to it	Contact information	Consent
<b>MAKE AN INFORMATION REQUEST</b>	Fulfil your information request	Contact information and enough information	Necessary to comply with a legal obligation to which we are subject
<b>SUBSCRIBE TO OUR E-NEWSLETTER</b>	So we can email information to you	Name and address	Consent
<b>ARE BEING INVESTIGATED BY THE ICO</b>	To establish whether a criminal offence has occurred and take any appropriate legal action	Information compiled during our investigation of an alleged offence	Necessary to perform our public tasks as a regulator
<b>PAY A FEE</b>	To communicate with you about the fee and any related issue	Contact and address information for your business, and DPO name if relevant	Necessary to perform our public tasks as a regulator
<b>REPORT A NUISANCE CALL OR MESSAGE</b>	Investigate and take regulatory action in line with our statutory duties	Phone number you received the call on and the first part of your postcode, contact information is optional	Necessary to perform our public tasks as a regulator
<b>ATTEND AN EVENT</b>	To facilitate the event and provide you with a good service	Contact information, organisation name, if offered a place, dietary requirements or access provisions. We may also ask for payment if there is a charge to attend.	Consent
<b>REQUEST OUR PUBLICATIONS</b>	So we can post information to you	Name and address	Consent

**KEY**

- PURPOSE OF PROCESSING PERSONAL DATA**
- the INFO WE NEED**
- LAWFUL BASIS for USING YOUR DATA**

For further information on how and why we use your personal data, including how long we keep it, your rights, who we share it with, and how you can contact us, please read our full privacy notice at: [ico.org.uk/privacy-notice](https://ico.org.uk/privacy-notice)

**ico.** Information Commissioners' Office

[UK ico Privacy Notice](https://ico.org.uk/privacy-notice)

## 3.9 Scientific Research

The GDPR provides certain allowances for data processing for scientific research purposes.<sup>55</sup> However, allowances or exemptions fall into the category of ‘derogations’ under the GDPR.<sup>56</sup> These derogations and their application will vary by member state, and will likely result in different legal requirements throughout the HBP and inside SPs. Not all member states have finished implementing GDPR derogations, so the extent of the differences remains to be seen. However, given the wide range of partners, and jurisdictional locations in the HBP, some variation is likely. This is an area that will require additional research and updates as the regulatory picture develops. This section first describes the exemptions generally, and then provides information on how the derogations apply in specific member states.

The current HBP policy on this point is that HBP partners must follow the policies of their home countries/institutions/data protection authorities. In line with the “origin based approach” all HBP partners are responsible of making certain that the data they submit, including where such collection and storage relies on the scientific research exceptions, conforms to the laws of their EU member state.

<sup>55</sup> GDPR Art. 89.

<sup>56</sup> In addition to Art 89, the GDPR also reserves the rights of Members states to introduce further conditions, including limitations, on processing of genetic, biometric, or other health related data.

### 3.9.1 General application of the GDPR to scientific research

Pursuant to GDPR Recital 33 and Article 89, if the purpose of data processing is for scientific research, certain exemptions are available regarding compliance with individual rights. These include: the [right of access](#) by the data subject, the [right to rectification](#), [restriction of processing](#), and the [right to object](#).<sup>57</sup> Additionally, the [right to erasure](#) or ‘the right to be forgotten’ does not apply when it “is likely to render impossible or seriously impair the achievement of the [scientific] objectives of the processing.”<sup>58</sup>

In addition to exemptions to individual rights, core principles of data protection including the principle of “[purpose limitation](#)” and the principle of “[storage limitation](#)” also contain exceptions for scientific research.<sup>59</sup> In short, the allowances for scientific research under the GDPR are substantial. However, for the exclusions to apply, the research must (1) be scientific, (2) meet ethical standards, and (3) apply appropriate safeguards.

- 1) The GDPR does not define the term ‘scientific research’, indicating only that the term should be applied in a broad manner.<sup>60</sup> Generally, the research must conform to accepted or standard scientific research requirements including applicable methodological and ethical standards.<sup>61</sup> The HBP clearly meets the definition of ‘scientific research’.
- 2) What is meant by ‘ethical standards’ is also left undefined in the GDPR. Given the substantial focus on ethics in the HBP, the ethical standards requirement is also likely satisfied. A separate opinion on this issue will be forthcoming.
- 3) In addition to meeting *scientific* and *ethical standards*, data controllers must adopt *appropriate safeguards* including technical and organisational measures, data minimisation, pseudonymisation, and anonymisation when possible.<sup>62</sup> Compliance with these safeguards are necessary for GDPR. Additionally, they are crucial for SPs and the HBP generally to take advantage of exemptions for scientific research.

For SP partners intending to rely on the scientific exemptions, they must be able to demonstrate that they meet the above elements in addition to having such an exemption available in their member state. In particular, having a plan for showing how the SP partners minimise and protect the data of research subjects.

### 3.9.2 Legal Basis for Scientific Research

As noted above, the GDPR broadly requires a legal basis for *any* processing of personal data.<sup>63</sup> For processing to be lawful, the processing party must have legitimate grounds for the duration of the processing.<sup>64</sup> For scientific research, the likely basis will be consent, public interest/official authority, or legitimate interest. The legal basis that is used will depend on the member state where data is collected and the policy of the university/institution acting as data controller.

For example, if an MRI is obtained for the purpose of treatment, that MRI *cannot* be automatically used for the purpose of research. This is the case even if the research takes place at the same hospital providing treatment. Further, if scientific research was not set as part of the purpose of collecting the data, such further processing or secondary use falls outside of primary purpose and

<sup>57</sup> GDPR Art 89(2). Reducing compliance obligations for Articles 15, 16, 18, and 21, respectively.

<sup>58</sup> GDPR Art 17(3)(d).

<sup>59</sup> See GDPR Art 5(1)(b) and GDPR Art 5(1)(e) respectively. See also GDPR Recital 33 and Article 89.

<sup>60</sup> GDPR Recital 159. See WP29 259 Rev. 01 (2018) 27-28. Expressing concern that scientific research may be applied too broadly and stretched beyond its logical meaning.

<sup>61</sup> WP29 259 Rev. 01 (2018) 28.

<sup>62</sup> GDPR Art 89(1).

<sup>63</sup> GDPR Art 6(1) (a-f).

<sup>64</sup> GDPR Art 6.

will exceed the consent provided for treatment. Thus, the further processing (research) is incompatible with the original purpose and violates the GDPR.

However, purpose specification is another area where the GDPR provides flexibility for scientific research. In particular, at Recital 33, the GDPR provides the following:

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.<sup>65</sup>

Unlike other areas where a specific purpose must be set at the beginning of processing, the flexibility for scientific research is aimed at addressing the problem that researchers do not always know what they are going to find when they start a research project. Therefore, setting a specific purpose, and limiting processing solely to that purpose, would be a significant limiting factor for projects such as the HBP. Recital 33 seems to indicate that ‘broad consent’ provisions will continue to be valid under the GDPR when ethical standards are in place.

If the purposes for data processing within a scientific research project cannot be specified at the outset, GDPR Recital 33 allows as an exception that the purpose may be described at a more general level. However, as noted by the European Data Protection Board (EDPB) if this exception is applied, it will be “subject to a stricter interpretation and requires a high degree of scrutiny.”

In summary, a best practice is to make the purpose of processing as specific as possible. However, this will not always be possible in HBP research. If the purpose is provided generally at the outset, participants should be provided with updates when processing becomes more specific. Updates could be provided by email or perhaps a dedicated website.

## 3.10 Consent in Scientific Research

In the HBP, consent will serve as the legal basis for the processing of personal data in many instances. The GDPR provides additional obligations for presenting, obtaining, and demonstrating valid consent. The core requirement is that the data subject (e.g. study participant, patient, etc.) is presented with a specific and genuine choice when consenting to have their data used for research purposes in the HBP. If the consent is uninformed, illusory, or coerced, it will be invalid and the data processing based on that consent will be illegal.

However, the GDPR also provides important accommodations/derogations for scientific research in the area of consent. Of particular relevance for the HBP, certain aspects of the *explicit consent* requirement is limited in the case of scientific research.



The HBP has a SOP on consent. However, the SOP will likely require further revision to comply with the GDPR. In particular, consent must be much more granular. The disclosure must make it clear to participants how their data will be used in the HBP and that they are submitting to research on a much broader basis than the local hospital or national health system where they obtain treatment. For some SPs, it may be necessary to obtain consent retrospectively.

### 3.10.1 Consent in research

The problem of obtaining and updating informed consent in scientific research is not necessarily novel to the GDPR. The process can be expensive, time consuming and complex, and even lead to

<sup>65</sup> GDPR Recital 33. Emphasis added.



participant fatigue or drop out. In order to reduce complexity and cost, many researchers apply ‘broad consent’ allowing for a variety of future research projects and objectives without requiring new consent.

As defined under the GDPR, consent must be a freely given, specific, and informed indication of the data subject’s wishes. This requires that a data subject has a genuine or real choice and control over their decision to consent. For instance, if consent for research is ‘bundled’ with medical treatment, it is unlikely that the consent will be valid.<sup>66</sup> Bundling consent for research to consent for treatment potentially puts pressure or influence on the data subject.<sup>67</sup>

The GDPR also specifies that where data will be processed for several functions, the ‘granularity’ requirement mandates that consent be provided from each of those function rather than broadly. Regarding consent for special categories of personal data (e.g. the processing of genetic data, biometric data, data concerning health, etc.) the GDPR *generally* prohibits such processing absent *explicit* consent or another legal basis under Article 9 (in addition to a legal basis under GDPR Article 6).

However, the GDPR provides an additional basis (i.e. in addition to explicit consent and vital interests) for processing special categories of data including scientific research under Article 9(2)(j) where:

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.<sup>68</sup>

At first blush, this basis appears to be quite extensive and read together with Recital 33 appears to confer wide latitude for researchers. Research articles on the matter point to expansive exceptions to the GDPR.<sup>69</sup> However, SP partners should not over-read the allowances provided for scientific research and should expect the EDPB to apply a strict interpretation and greater scrutiny where the HBP relies on such exceptions.

Further, the EDPB provides that the exceptions are limited and that “...Recital 33 does not disapply the obligations with regard to the requirement of specific consent.”<sup>70</sup> That is, researchers cannot ignore key data protection principles. Even if two of the six principles of data protection are in a sense reduced for scientific research, the other four (lawfulness, fairness and transparency, data minimisation, accuracy, and integrity and confidentiality) remain fully applicable.<sup>71</sup> Further, the ‘new’ accountability principle will also apply.<sup>72</sup>

On that basis, the EDPB provides some points that should be considered by researchers. First, if the purposes of the research cannot be fully specified, the controller is obligated to include additional safeguards. For instance, if only general information is provided when the consent is obtained, this should be updated when more information on the purposes of the research becomes available. As the research advances, additional consent for subsequent steps may also be appropriate. A more general consent also requires that attention be given to all applicable ethical

<sup>66</sup> WP29 259 (2018), 5.

<sup>67</sup> GDPR Art 7(4). GDPR Recital 43. WP29 259 (2018), 6-7. Evaluating the impact of an imbalance in power.

<sup>68</sup> GDPR Art 9(2)(j). However, for the exception to be applicable, it must be adopted by a member state as part of the derogations under GDPR Art 89. Determining or defining Safeguards are also left to the member states. Mahsa Shabani & Pascal Borry ‘Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation’ (2017) 26 European Journal of Human Genetics volume 149, 154.

<sup>69</sup> Kärt Pormeister, ‘Genetic data and the research exemption: is the GDPR going too far?’ (2017) 7:2 International Data Privacy Law 137, 139-140. Available at <<https://doi.org/10.1093/idpl/ix006>>.

<sup>70</sup> WP29 259 (2018) 28.

<sup>71</sup> GDPR Art 5(1) (a, c, d, and f) respectively.

<sup>72</sup> GDPR Art 5(2).

standards as normally applied within the scientific research. In addition to providing updates and following ethical standards, the GDPR requires that the scientific research put in place appropriate safeguards including data minimisation, anonymisation, and data security.<sup>73</sup> The next section considers practical steps for including this guidance in the HBP.

## Practical Steps and Impact on the HBP

Based on the GDPR and EDPB guidance, consent in scientific research under the GDPR should take account of the following:

- Data subjects must be provided with clear information regarding the identity of the controller, purposes for data processing, and information on sharing of data with third-parties.
- When consent is the legal basis for conducting research, it must be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. For example, if you are basing consent on Clinical Trials Regulation, you should also obtain consent for data protection purposes.
- Consent must be obtained on an “opt-in” or other active basis.
- At the time of consent, data subjects must be provided with clear information regarding the identity of the controller, purposes of data processing/research, and relevant information on sharing of data with third-parties.
- Consent should be as specific and granular as possible. Make it clear that data submitted to the HBP will be made available to researchers outside of the immediate hospital and the EU more generally.
- Document consent (i.e. demonstrated and verifiable through records).
- Participants (or legal guardians when the data subject cannot provide consent) have the right to [withdraw consent](#).



### 3.10.2 Impact on Broad Consent

The GDPR appears to allow the continued use of so-called “broad consent” for scientific research. However, the EDPB subscribes to the view that access to such consent should be updated on continual basis. In the HBP, we should consider ways of providing updates to consent and other means to provide participants with results and progress of research. To avoid participant fatigue, SP partners should consider developing a tiered approach. For example, one track would require ‘rolling’ or new consent for each stage of the research. A second track would allow the data subject to consent to not obtaining further consent requests.

### 3.10.3 Withdrawal of consent

In providing specific conditions and means for evaluating consent, the GDPR states that “[i]t shall be as easy to withdraw as to give consent.”<sup>74</sup> Even in the case of scientific research, data subjects have the right to withdraw their consent.<sup>75</sup> The GDPR does not provide an exemption to this

<sup>73</sup> GDPR Art 89(1).

<sup>74</sup> GDPR Art 7(3).

<sup>75</sup> *ibid*.



requirement for scientific research.<sup>76</sup> Therefore, if HBP controllers obtain a request to withdraw consent, they must generally act on this request and delete the personal data. This will require that HBP Platforms build in or include this functionality.

#### Non-data protection consent requirements

Data collected from human beings must have been collected according to the ethical principles governing research in the EU. Where the data were collected as part of the HBP work, compliance with the ethical principles will have been checked during the Ethics Review.

Further, data from humans that was collected outside the HBP has to comply with the same standards. Evidence must be provided that:

- 1) The data subject consented to the procedure undertaken to collect the data,
- 2) The data subject consented to the use of the data for the research purposes that it is to be used for, and
- 3) Where no consent for data sharing is available, the re-use of the data must be legal according to EU data protection legislation.

These principles apply to both experimental data collected from volunteers and to medical and patient data. The ethics approval to collect human data will normally be provided by a competent authority such as a national or regional research ethics committee. The research underlying the data must either have been conducted in a European country and have received such approval or it has to comply with the principles and be in a position to receive approval, if it were to be undertaken in a European country. In countries where special authorisations are required, it is assumed that this has been collected, prior to the onset of data sharing (e.g. special authorisation from la commission nationale informatique et libertés (CNIL) in France).

In order to help PIs, the HBP has developed a [Standard Operating Procedure on Informed Consent](#). This SOP contains the minimum standards that need to be met for research to count as acceptable. Local research ethics committees or other relevant authorities may require stricter standards in line with local regulations. The informed consent SOP should provide Data Custodians of data collected outside of the EU with an indication of whether their ethics processes are equivalent to European standards.

Data that do not fulfil these criteria should not be registered or used in the HBP digital research infrastructure.



The data protection officer is working on an updated opinion on consent under the GDPR. A link will be added when the opinion is finalised.

## 3.11 Relevant Scientific Research (SR) Derogations by Member State

For the HBP as a whole, the derogations are generally positive and enhance the ability to conduct scientific research, when applicable. However, they also present a significant challenge to creating one policy that can be adopted across the project.

<sup>76</sup> WP29 259 Rev. 01 (2018) 28-29.




The chart below gives an overview of the status of Scientific Research (SR) derogations and GDPR across the EU based on research from Bird & Birda leading international law firm.<sup>77</sup> This evaluation is ongoing and derogations by member states are still under determination in some countries. Therefore, SPs should contact local DPOs to confirm SR derogations and requirements under national law. The chart **that follows is for informational/status purposes only, and cannot be taken as legal advice, authorisation, or general HBP policy.**

Country	GDPR Adopted/ Finalised	Relevant Scientific Research (SR) Derogation
Austria	Yes	All other data processing activities for scientific, historical or statistical purposes require (i) a specific statutory authorisation, (ii) the consent of the data subject or (iii) approval by the Austrian Data Protection Authority. Since these provisions are quite restrictive, special regulations for certain areas (especially health-care and pharma sector) are currently in legislation process.
Belgium	No. In consultation	N/A
Czech Republic	No. In consultation	N/A
Denmark	Yes	§10 permits processing of special category data and data related to criminal offences for statistical or scientific purposes when necessary for reasons of substantial public interest and if necessary for the research; §11(3) permits processing of personal identification numbers by private organisations for statistical or scientific purposes; §22(5) restricts data subjects' rights in relation to statistical or scientific purposes.
Finland	No. In consultation	Proposed Data Protection Act includes derogations and safeguards in accordance with Article 89 GDPR. Processing for scientific, historical or statistical purposes is permissible as long as the safeguards in Article 89 GDPR and the proposed Data Protection Act are met.
France	No. In consultation after constitutional appeal  Unclear on SR.	The New Data Protection Act adds a provision on the data subjects' rights in case of processing for <b>archiving purposes</b> . The right of access, the right to rectification, the right to restriction of processing, the right to data portability and the right to object do not apply for this type of processing.
Germany	Yes	§27 FDPA permits <b>processing of sensitive data without consent</b> : - for scientific or historical research; and - for statistical purposes  if the processing is necessary for these purposes and the data controller's interest to process data significantly outweighs the data subject's interest.  The data controller must apply certain "suitable and specific" measures.

<sup>77</sup> Based primarily on the international law firm Two Birds 'GDPR Tracker' available here <https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker>.



		<p>Provision also restricts data subjects' rights in the context of processing for research and statistical purposes, and sets out requirements for the publication of such data.</p> <p>§32-37 FDPA also contain other (general) restrictions of data subjects' rights on the basis of Art. 23 GDPR.</p>
Hungary	No. In consultation	N/A
Ireland	Yes.	Under section 42 of the Act, personal data may be processed for (a) archiving purposes in the public interest; (b) scientific or historical research purposes; or (c) statistical purposes, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects.
Italy	Amended current act to comply with GDPR?	<p>Amended Section 99 IDPA, allows personal data to be processed; stored; &amp; transferred to another controller after the normal period for processing of personal data and even after the termination of the main data processing if these processing will be carried out for scientific, historical or statistical purposes as well as at archiving in the public interest.</p> <p>Amended Section 106 IDPA - the Italian DPA is to promote rules for professional and ethical conduct for processing for statistical purposes or for scientific research. Rules to apply both to public and private bodies, scientific societies and professional associations. Aim of the guidance is to identify adequate guarantees for the rights and freedoms of the data subject in accordance with Article 89 GDPR.</p> <p>Amended Section 110 IDPA: possible to carry out scientific and medical research, using special categories of data, without consent in certain circumstances.</p> <p>Amended Section 110-bis IDPA: ability for the Italian DPA to authorise secondary uses of special category data for scientific and statistical research, in situations where it is impossible or would involve a disproportionate effort to inform all data subjects. Does not apply to genetic data.</p>
Netherlands	Yes	Article 42 GDPR Execution Act provides that where processing takes place solely for scientific or historical research purposes, or statistical purposes, the controller may declare articles 15, 16 and 18 of the GDPR inapplicable. Data subjects will not have rights of access, rectification or restriction of processing for these data.
Norway	Yes	<p>Special categories of personal information may be processed without additional consent (e.g. broad consent). This applies to the following purposes:</p> <ul style="list-style-type: none"> <li>• Archival purposes in the public interest</li> <li>• Purpose related to scientific or historical research</li> <li>• Statistical purposes</li> </ul> <p>The exception requires an analysis/balancing of the public policy interests and the fundamental rights of the individual. Medical professionals/researchers must seek guidance from a DPO or other professional to conduct a risk/data protection assessment.</p>
Poland	Yes. SR and other derogations ongoing.	N/A
Spain	No. In consultation?	<p>Article 25 - processing of personal data for statistical purposes:</p> <p>a) will only be lawful only if the information is required by an EU rule or by the statistical programming rules;</p>

		<p>b) Spanish Government Statistics Act: processing of special category data for statistical purposes must be based on express and voluntary consent of the data subject;</p> <p>c) If statistical secrecy guarantees under Spanish legislation apply, competent bodies for the public statistical function can deny data subject rights in Articles 15 to 22 of the GDPR .</p> <p>Article 26 - processing of personal data for archiving purposes in the public interest is subject to the Spanish Historical Heritage Act and other related regulations.</p> <p>Draft Bill does not provide information about the processing for scientific or historical research purposes.</p>
Sweden	Yes	N/A
Switzerland	N/A	N/A
UK	Yes	<p>Sched.1, part 1, §4 Processing of special category data and criminal offence data for archiving purposes, scientific or historical research purposes, or statistical purposes permitted if:</p> <ul style="list-style-type: none"> <li>• in accordance with GDPR (Art.81) (use of t.o.m.s and data minimisation; anonymise if possible; pseudonymise if possible); and</li> <li>• must not be likely to cause damage or distress; must not be used for measures or decisions with respect to a particular data subject unless is approved medical research (s.19); and</li> <li>• is in the public interest.</li> </ul> <p>Exemptions from data subject rights (access; rectification; restriction; portability; right to object) where processing meets conditions set out in Art.89 (1) &amp; s.19 DP Act; and</p> <ul style="list-style-type: none"> <li>• compliance would prejudice the ability to achieve the purposes of the research/ statistics/ archiving; and</li> <li>• for research/ statistics: the results must not be made available in identifiable form.</li> </ul>
 <p>The HBP DPO plans to contact local DPOs to update and finalise the above table. SPs should consult with their local DPOs and national experts to determine adoption in their member states.</p>		

### 3.12 Data protection by design and default

Data protection by design and data protection by default require that data controllers design and implement systems that safeguard the rights of data subjects.<sup>78</sup> For the HBP, this means integrating data protection requirements, including the [principles](#), into all aspects of ICT use and development from training and design to maintenance.

The GDPR does not prescribe a specific formula or method for meeting data protection by design and data protection by default requirements. Like other areas of the GDPR, it requires applying a risk-based approach and will depend to some extent on the processing taking place.

As a starting point, SP partners designing any system should determine whether that system will process personal data or whether data may become personal as a result of the processing (re-identification). If the answer is yes, a DPO or data protection expert should be added as a

<sup>78</sup> GDPR Article 25 and Recital 78.

stakeholder to the project. Furthermore, at the earliest phases, developers should consider how they might incorporate data protection by design elements evaluated in the next section in addition to taking account of the [data protection principles](#).

All HBP SP partners are required to design, develop, and operate their services employing “privacy by design” and “privacy by default” principles. Below are key starting points:

- **Pseudonymisation:** Pseudonymising personal data as soon as possible. By applying pseudonymisation, encryption, and aggregation of personal data, the risk of loss or misuse is significantly reduced. SPs should apply these techniques whenever possible.
- **Data [minimisation](#):** Reduce the amount of personal data collected and processed to what is: (1) lawful and (2) strictly necessary. Do not collect unnecessary or excessive information for the [purpose](#). Delete data when storage is no longer required for the purposes. For example, if personal data such as email addresses have been collected for an HBP event, they should be deleted after the event if they are no longer needed and the purpose for which they were collected (attendance) has been completed. If you do not need GPS/location data to complete the purpose, do not collect it.
- **Purpose limitation:** Design organisational or technical means that allow users to set a purpose for the data collection.
- **Organisational measures:** Adopt internal policies aimed at data protection by design. In addition to the DPM at a project level, SPs should consider the internal steps they might take to improve data protection in their practices. For example, adding data protection to their [risk assessment](#). Create clear requirements for documentation.
- **Technical measures:** Use encryption, access control, and other measures to limit the risks to data subjects. For example, avoid linkability between different data sets. Create procedures to split database tables, distinguish between components, and create different access requirements for areas with sensitive personal data. Take steps to limit the creation of a complete profile of a data subject.
- **Deletion/destruction:** Once the purpose of data collection has been completed, design processes for deletion. Further, follow best practices on data deletion and destruction.
- **Transparency:** Make it clear for data subjects what data are being processed, who is processing the data, why it is being processed, how, and how long will the data be kept. Does the information we provide given potential data subjects enough information about what we do and how we will use their data? This information could be contained on a website, as part of a privacy policy, in an informed consent form, etc.
- **Data protection by default:** Configure all settings to the most privacy-friendly ones.



## 3.13 Individual Rights

HBP partners must support compliance with certain individual rights. This is an area where EU member states have some ability to derogate or deviate from the GDPR scientific research. Derogations are noted herein.

### 3.13.1 *The right to be informed*<sup>79</sup>

A key transparency requirement in the GDPR is the individual's right to be informed regarding data collection and use. HBP controllers must be able to provide:

- 1) Purposes for processing personal data,
- 2) Retention periods for that personal data,
- 3) Information on the parties the data will be shared with (e.g. processors).

This information must be available to data subjects when data are collected. If a data subject requests the above information, it must be provided within a reasonable period. The UK DPA sets this period at one-month. Furthermore, the information should be provided in a concise, transparent, intelligible, easily accessible manner using clear and plain language. As provided above in the section on [documentation](#), this will require keeping complete and updated records. The EDPB has adopted detailed guidelines on transparency available [here](#).

#### **The right to be informed in the HBP**

A good starting point for meeting this requirement is with the privacy policy provided at the time of data collection. SP controllers should include the following information in their privacy policy/website/informed consent:

- Name and contact details of the HBP/SP/CDP partner or other data controller;
- A link to PORE and the HBP DPO contact page;
- The purpose of processing;
- The lawful basis of the processing ;
- Legitimate interests for the processing (if used as a lawful basis);
- Right to withdraw consent (if used as a lawful basis);
- The categories of personal data obtained;
- Information on transfers of the personal data to any third countries;
- Retention periods;
- Rights available;
- Source of personal data (if applicable); and
- Information on automated decision-making or profiling (where applicable).

In providing the above information, HBP controllers should make their privacy disclosures easy to understand and as concise as possible. In addition to using plain language, consider using dashboard notices, icons, or even drawings if appropriate. See [UK ico Privacy Policy](#) above.



<sup>79</sup> GDPR Articles 13 and 14. See Further GDPR Art 12 and EDPB, 'Guidelines on transparency under Regulation 2016/679' (29 November 2017).




### 3.13.2 The right of access<sup>80</sup>

The right of access gives data subjects the rights to obtain certain information including:

- Confirmation that the HBP/SP/CDP partners are processing their personal data.
- A copy of the data subjects personal data from an HBP controller (generally within one month of the request) in a commonly used electronic format.
- In almost all cases, the information should be provided without charging a fee. If you intend to charge the data subject for obtaining their personal data, contact your local DPO or the HBP DPO for guidance.

In addition to providing a copy of personal data, SP partners should also be prepared to provide the information regarding the purpose of processing, personal data collected, retention periods, etc.). If this information has already been provided in a privacy notice, a link to that notice or policy can be provided along with a copy of the record.



The GDPR does not provide a format or procedural requirements for the request. The HBP policy is therefore to accept any mode of communication including requests made by email, letter, the PORE or the DPO request page. To the extent possible, a record or log of the request and its resolution must be kept. For help in providing the required information, all SPs and CDPs should contact the HBP DPO.

	<b>Scientific Allowance:</b> EU member states have the option of adopting an exception to ‘the right of access’ for scientific research when the requirements of Art. 89 (1) (see <a href="#">Scientific Research</a> Section) have been met.
--	---

### 3.13.3 The right to rectification<sup>81</sup>

The right to rectification gives data subjects the right to correct inaccurate personal data. Generally, this includes data that is incorrect or misleading. The greater the impact of the inaccuracy on the data subject, the higher the burden on the controller to correct such information. For example, information that a patient has a medical condition should be corrected if the condition is successfully treated. This right is closely tied to the ‘[accuracy principle](#)’.<sup>82</sup>

SP partners must have processes to correct personal information. If it is difficult or impossible to correct information, the SP partners should also have a means for deletion.

<b>The right to rectification in the HBP</b> SP partners must have a processes to correct personal information. If it is difficult or impossible to correct information, the SP partners should also have a means for deletion.	
	
	<b>Scientific Allowance:</b> EU member states have the option of adopting an exception to ‘right to rectification’ for scientific research when the requirements of Art. 89 (1) (see <a href="#">Scientific Research</a> Section) have been met.

<sup>80</sup> See GDPR Art 15. See further Recitals 63, 64.

<sup>81</sup> GDPR Art 16.

<sup>82</sup> See further GDPR Articles 5, 12, 16 & 19.

### 3.13.4 The right to erasure ('right to be forgotten')<sup>83</sup>

The right to erasure (also known as 'the right to be forgotten') provides data subjects with the right to have their data erased. Once a request to erase data has been received, the data can no longer be used for any purpose.

#### The right to erasure in the HBP

Data should **generally be deleted** when:

- The purpose for which the data was collected has been completed;
- Consent has been withdrawn;
- The legitimate interest relied on is no longer adequate to justify processing; or
- Data were processed unlawfully.

Therefore, HBP/SP controllers must have processes in place to meet such requests. As a starting point, HBP controllers should:

- Have a process in place to respond to such requests;
- If data have been shared, have a processes to contact controllers/joint controllers/or processors for deletion; and
- Have appropriate methods to delete or erase data including from backup systems (i.e. rewrite over time).



**Scientific Allowance:** EU member states have the option of adopting an exception to 'right to erasure' for scientific research when applying the right "...is likely to render impossible or seriously impair the achievement of the objectives of that processing..." See GDPR Article 17(3)(d) and the [Scientific Research](#) section for further details.

### 3.13.5 The right to restrict processing<sup>84</sup>

Data subjects have the right to request that their data be restricted in some circumstances. The right is essentially an alternative to requesting that personal data be deleted. Data controllers retain the right to store such data, but not to process the data. In essence, the data are taken out of circulation. Circumstances in the HBP might include:

- A patient contests the accuracy of their personal data.
- A controller no longer needs the data, but is requires a record of the data to defend a legal claim.
- An individual has objected to the use of personal data, and the SP is attempting to determine whether they have legitimate grounds to continue processing the data.

#### The right to restrict processing in the HBP

SP partners must implement technical and organisational measures to comply with requests to restrict processing. These could include temporarily moving the data to another processing

<sup>83</sup> GDPR Art 17 & Recital 66.

<sup>84</sup> GDPR Art 18 and Recital 67.

system, making the data unavailable to users. In the case of the MIP or the NIP, when possible, temporarily removing data from the Platforms.

Like the other individual rights, the request can be made verbally or in writing. SPs should respond to requests within one month. A request to restrict processing can be refused where it is manifestly unfounded or excessive. Similarly, SP partners can charge a reasonable fee in some circumstances. However, any refusal or fee will require justification.



**Scientific Allowance:** EU member states have the option of adopting an exception to ‘right to restrict processing’ for scientific research when the requirements of Art. 89 (1) (see [Scientific Research](#) Section) have been met.

### 3.13.6 The right to data portability<sup>85</sup>

The right to data portability gives data subjects the right to request a copy of their personal data they have provided to a controller in a format they can move or take with them to another service. This may include easily identified information such as email address or contact details. It may also include traffic or location data, data processed using connected objects such as wearable devices. The purpose of the provision is to allow users to move from one IT environment to another.

Data should be transmitted securely in a commonly used machine-readable format. Only controllers are required to provide the data. The right is further limited to data processed on either the [legal basis](#) of consent or performance of a contract and only includes personal data as defined above.

### 3.13.7 The right to object<sup>86</sup>

Data subjects may object to personal data processing in a variety of circumstances. The breadth of the right will to some extent depend on the purposes of the data processing. For example, in the case of direct marketing/profiling the right to object is effectively absolute. However, in other cases, the objection must be balanced against other rights in other situations. When data are processed for the purpose of scientific research, the right to object and stop processing is limited. The GDPR provides that the right to object is available, “...unless the processing is necessary for the performance of a task carried out for reasons of public interest.”<sup>87</sup>

#### The right to object in the HBP

In the HBP, data collected and processed for research purposes will outweigh an objection when it is necessary to carry out the task. However, SPs should take care not to over-apply this exception. For example, even if most of the personal data subject to the request is part of the scientific purpose, when the data are also used for other purposes outside of scientific research, the right will still apply.



<sup>85</sup> GDPR Art 20. See also EDPB, ‘The right to data portability Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01’

<sup>86</sup> GDPR Art 21. See also GDPR Articles 6, 12, 89 and recitals 69 and 70.

<sup>87</sup> GDPR Art 21(6).



**Scientific Allowance:** EU member states have the option of adopting an exception to ‘right to object’ for scientific research when the requirements of Art. 89 (1) (see [Scientific Research](#) Section) have been met. See also: GDPR Article 21(6).

### ***3.13.8 Rights in relation to automated decision making and profiling<sup>88</sup>***

Automated individual decision-making is a decision made by automated means without any human involvement. This includes making decisions such as whether or not to provide a loan, and making recruitment or employment decisions. The GDPR restricts solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. In the HBP, several SPs use machine-learning and big data. However, based on the Ethics Rapporteur one-pagers, it does not currently appear that any SPs are using algorithms to make automated decisions in the manner prohibited under the GDPR.

## **3.14 Data Protection Officer<sup>89</sup>**

The General Data Protection Regulation (GDPR) requires the designation of a Data Protection Officer (DPO) in some circumstances. Given the scope and categories of personal data processed in the HBP, the project has appointed a DPO. The DPO works with HBP partners within SPs and CDPs to facilitate compliance with the GDPR.

The DPO is a professional in the field of data protection and assists with monitoring of internal compliance and data protection obligations across the HBP in addition to acting as a contact point for data subjects and the supervisory authorities. Additionally, the DPO focuses on increasing accountability to data subjects across the HBP. 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. The DPO has created a confidential contact point as shown below and available [here](#).

<sup>88</sup> GDPR Articles 21 and 22. See also WP29, ‘Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)’. Endorsed by the EDPB.

<sup>89</sup> GDPR Articles 37-39. See also WP29, ‘Guidelines on Data Protection Officers (‘DPOs’) WP 243 rev.01’. Endorsed by the EDPB.

UiO University of Oslo

Bokmål Nynorsk

Nettskjema

Surveys, registrations and orders

Help Kevin McGillivray Log out

Home My forms HBP Data Protection Officer

HBP Data Protection Officer

Change title

Open for submissions?

The form is open

Close Advanced

Last modified

7. May 2018 10:24

by Kevin McGillivray


View Form builder Settings Permissions Collect responses See results

Overview of the form's submissions

HBP Data Protection Officer - refno 2674522

Delivered on 23. February 2018 14:37

Contact the Data Protection Officer (DPO)



Human Brain Project

Name (Optional) \*

Kevin

E-mail (If anonymous, leave blank)

Mcgillike@yahoo.com

What is your relation to the HBP?

Partner/Researcher

Describe relevant work areas (if any)

Privacy

Issue specification/Description


Breach

Do you require a response?

Note: If you are submitting your concern on an anonymous basis the DPO cannot provide a response.

Yes

See recent changes in Nettskjema (v362\_0rc2)



Terms

Terms of use and privacy

Nettskjema uses cookies

Contact information

Contact Nettskjema

Responsible for this service

Web Department – USIT

## DPO Contact:

The DPO has created a confidential contact point [here](#).

The DPO is also available via email ([kevin.mcgillivray@jus.uio.no](mailto:kevin.mcgillivray@jus.uio.no)) or as provided on the [HBP webpage](#).

SP1

SP2

SP3

SP4

SP5

SP6

SP7

SP8

SP9

SP10

SP11

SP12

D12.4.1 (D78.1 D114) SGA2 M1 ACCEPTED 190723

PU = Public

23 Jul 2019


Page 47 / 70

## 3.15 Documentation Requirements

The GDPR explicitly requires that the HBP/SPs/CDPs data controllers document data processing activities.<sup>90</sup> In addition to providing practical information such as the contact details of the parties responsible for data processing, the HBP partners must maintain records of the purposes of processing, a description of data types, information on data sharing and data transfers, data retention schedules, data security and organisational measures, among others.

To meet this requirement, the DPO and the DGWG undertook a “data mapping” survey designed to collect the information necessary to comply with GDPR requirements. This survey has also been used to provide a more granular and complete ‘map’ of the personal data processed in HBP.<sup>91</sup> The second objective is to review our policies and procedures for compliance with the GDPR more generally. In particular, this requires a better understanding of our data flow including the location of personal data, an assessment of existing contracts and privacy policies, Privacy Impact Assessments (PIAs), and Data Protection Impact Assessments (DPIAs), where available.

An excel sheet (shown below) has been created for each SP to record and manage documentation requirements. SP partners are responsible for keeping the record accurate within their institutions. They are also required to provide the DPO and Ethics Support (WP12.4) with updates.

 Human Brain Project		Controller (SP#)			
Name and contact details		Data Protection Officer (if applicable)		Representative (if applicable)	
Name		Name		Name	
Address		Address		Address	
Email		Email		Email	
Telephone		Telephone		Telephone	
Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	Link to contract with processor

In addition to ensuring compliance with an audit, having a clear overview and complete records is necessary for data breach reporting, in addition to complying with other aspects of the GDPR such as the rights of individuals to request erasure or data portability.

Documentation in the HBP
All SP partners are required to keep documentation of their data processing activities. SP partners must also update the HBP DPO on data processing within the project.
<div> <div>SP1</div> <div>SP2</div> <div>SP3</div> <div>SP4</div> <div>SP5</div> <div>SP6</div> <div>SP7</div> <div>SP8</div> <div>SP9</div> <div>SP10</div> <div>SP11</div> <div>SP12</div> </div>

## 3.16 Data Breach<sup>92</sup>

Pursuant to the GDPR, a data breach includes “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.”<sup>93</sup> The GDPR requires all organisations to report certain data breaches to the relevant supervisory authority. This must generally occur within 72

<sup>90</sup> GDPR Art 30.

<sup>91</sup> This will also contribute to other GDPR requirements including accountability. GDPR Art 5(2).

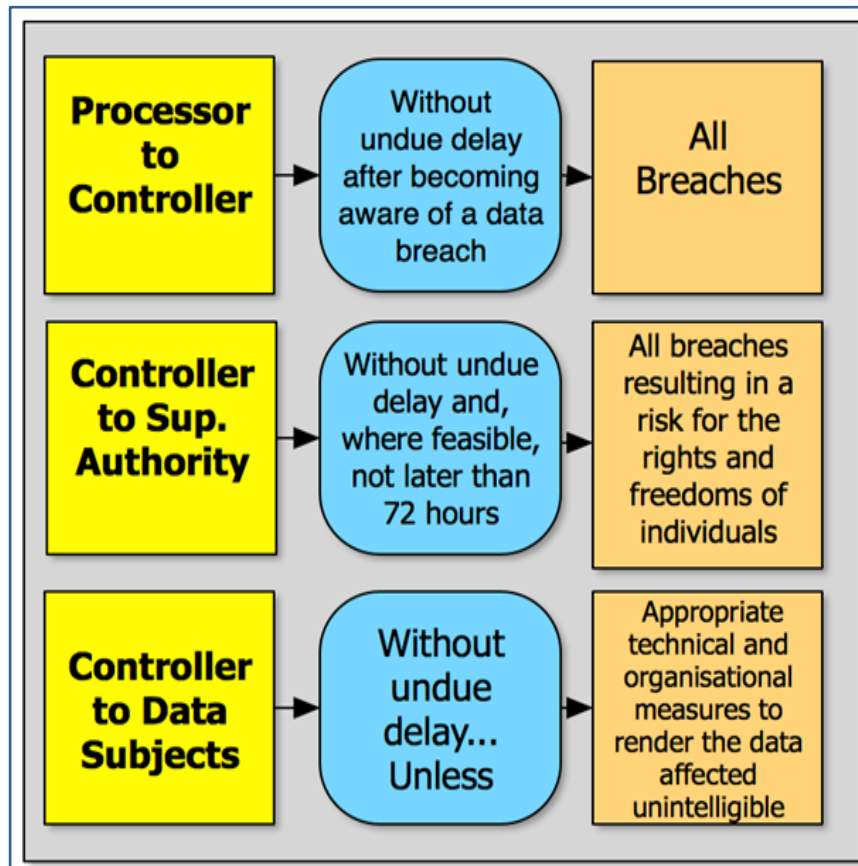
<sup>92</sup> GDPR Articles 33-34. Recitals 75, 85-88. WP29 guidelines on personal data breach (endorsed by the EDPB) available here [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612052](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052).

<sup>93</sup> GDPR Art4(12).



hours. Therefore, SP partners must have reporting practices in place. HBP partner stakeholders will generally include a local data protection officer (DPO) and computer emergency response team (CERT).

The following Figure provides an overview of the GDPR data breach requirements.



The SP partners must also inform the HBP DPO of any data breach. In addition to having a means of reporting, the SP partners must also have robust breach detection capabilities and the ability to recognise a data breach. In some cases, SP partners will have to inform data subjects of the breach.

Examples of potential data breaches in the HBP:



- Unauthorised access to an HBP Platform.
- Sending personal data to an incorrect recipient. This might be done with an email or sharing a link to a document.
- A lost or stolen laptop containing personal data. If properly encrypted, the SP partners may escape reporting the data subject, but must report the loss to their local DPO/CERT and the HBP DPO.
- A loss of availability, confidentiality, or integrity of personal data. For example, if an SP partner is subject to a ‘ransomware’ attack and no longer has access to data.

#### Data Breach in the HBP

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 \(PORE\)](#).

A submission should include at least the following information:

- Name of the reporting individual and means of contacting them (email)
- Description of breach

<ul style="list-style-type: none"> <li>• Cause of the data breach</li> <li>• Dataset affected</li> <li>• Description of how it was identified</li> </ul> <p>Upon submission to the <a href="#">PORE</a>, the data breach will be brought to the attention of the Ethics Manager and Ethics Support team.</p> <ul style="list-style-type: none"> <li>• An immediate notification will be sent to the DIR.</li> <li>• Where required, further investigations will be undertaken to clarify the exact nature of the breach and its consequences.</li> <li>• Ethics Support and the DIR will identify the relevant supervisory authority and report the breach to this authority if required.</li> </ul>	
	
	<p>A data breach may require an internal audit. The Data Governance Working Group (DGWG) is currently working on procedures for internal audit. The DPM will be updated when such procedures are finalised.</p>

## 3.17 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a tool for building and demonstrating compliance with the GDPR. DPIAs employ a systematic process for assessing the impacts of the processing of personal data and the effect that processing has on the fundamental right to privacy of the data subject. The controller has the primary responsibility for performing the DPIA. A DPIA should take place “prior to the processing” of personal data. The EDPD makes it very clear that the DPIA should take place early, often, and continuously.

There is no set formula for carrying out a DPIA. The French DPA, CNIL, has provided helpful guidance on the matter. According to the CNIL, the compliance approach requires: (1) compliance with fundamental rights and principles, and (2) management of the data security risks. Compliance with the GDPR requires meeting both of these aspects as demonstrated in the following CNIL graphic.



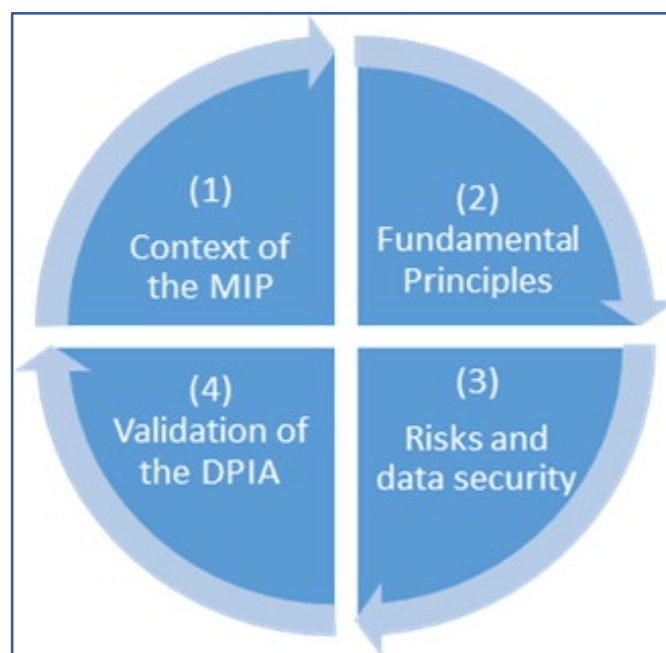
The DPIA process should “be continuously reviewed and regularly re-assessed.” In other words, this is not a one-off exercise. This is particularly necessary when creating new technologies and infrastructures such as the MIP or the NIP, but does not exclude processing in other HBP SPs.

In some cases, a DPIA is voluntary while in others it is mandatory. Data processing operations in the HBP more generally have the potential to “result in a high risk to the rights and freedoms of natural persons.” As a result, HBP partners are obligated to perform DPIAs in several areas. In particular, HBP Platforms, and more generally the scope and subject matter of research in the SPs, contain special categories of personal data including personal medical records.

### 3.17.1 Carrying out a DPIA: Methodology

As a point of departure, DPIA requirements are flexible and intended to be scalable to the processing operation. That is, SPs will have some flexibility in determining methodologies, structure, and the form of the assessment. However, the DPIA must be a “genuine assessment of risks” which can then be addressed by the controller. Moreover, given the scope of the project, scale of processing activities, and overall level of financing and sophistication, the HBP partners can expect to be held to a high standard in its DPIA analysis.

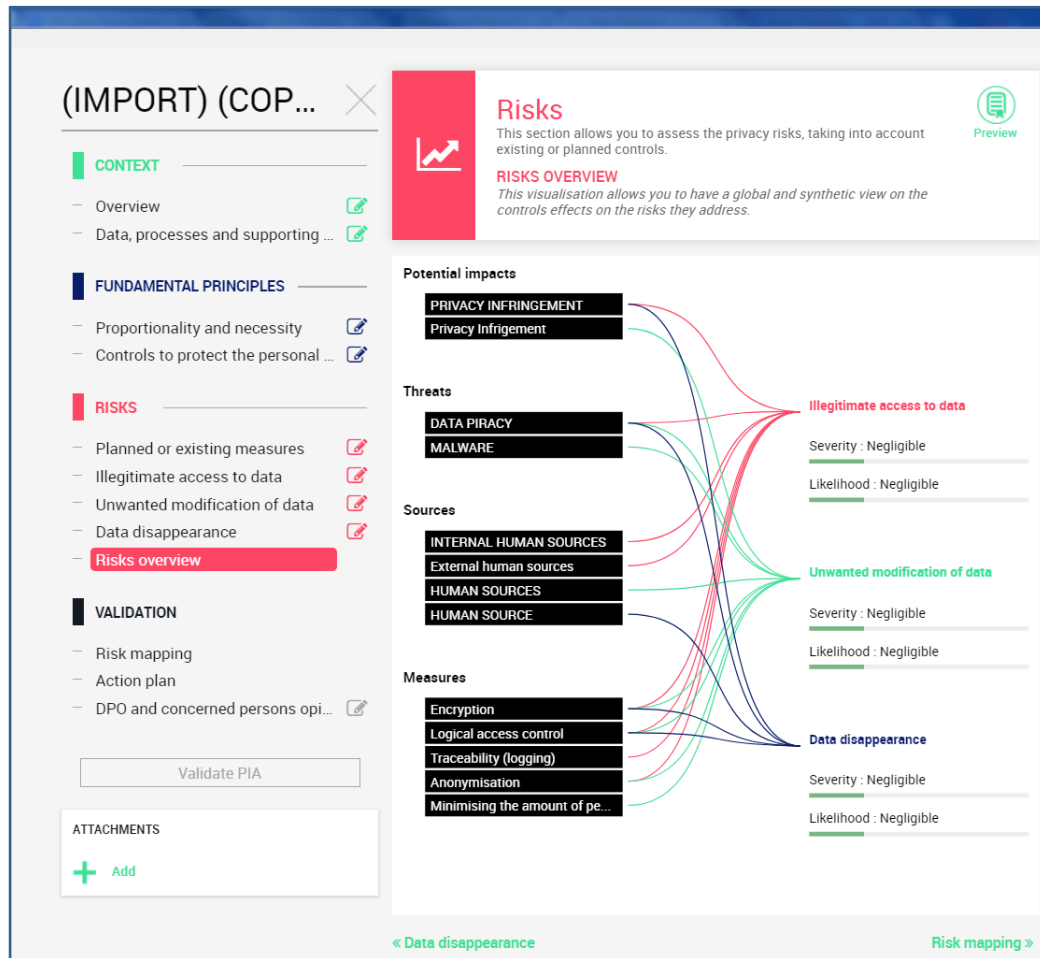
The CNIL has created a method supported by open source software tools for conducting DPIAs. The CNIL guidance incorporates the requirements of the GDPR and the WP29 Opinion on DPIAs. The CNIL method can be combined with other methods including the recently released ISO DPIA method and the method provided by the UK. Although SP partners may apply another method, the HBP DPO recommends applying the CNIL DPIA. The graphic below shows the CNIL method as applied to the MIP.



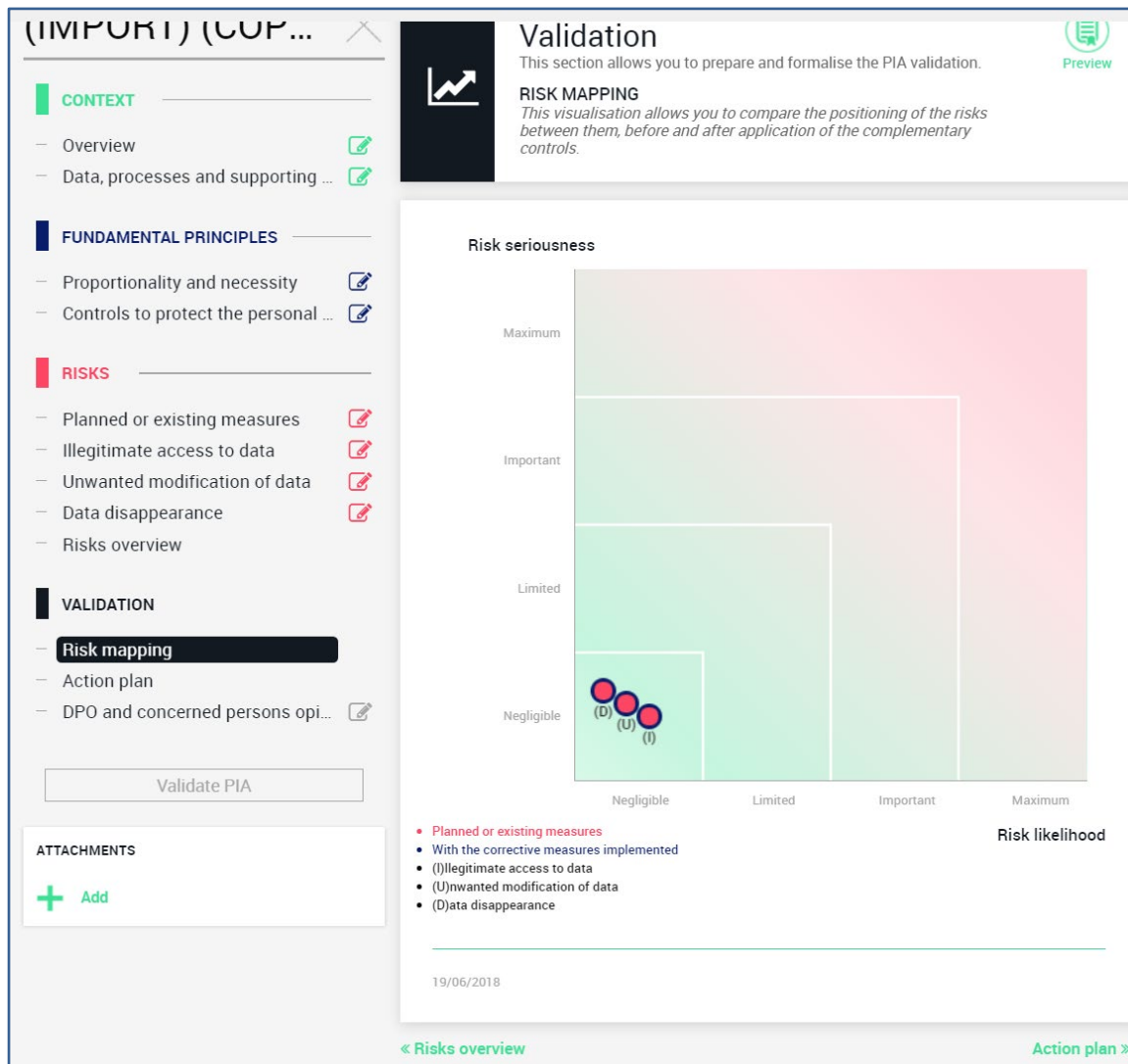
- 1) **Context:** This step requires defining the context of the data processing operation. This includes an assessment of the nature, scope, and purpose of the processing operation. SPs must also be able to identify data controllers and data processors, and evaluate their roles and responsibilities in processing operations. Further, SPs should be able to describe in detail the data collected, recipients and storage durations, and provide description of the processes from collection to erasure.
- 2) **Fundamental Principles:** This step requires analysis of compliance with the fundamental privacy principles set out in the GDPR. The “assessment of the risks to the rights and freedoms of data subjects” requires identifying controls selected to comply with informational and other the rights of the data subject such as data portability, rectification, erasure, restricted processing, among others. Further, controls to meet consent requirements, international transfers of data, data processing agreement requirements.
- 3) **Risks and data security:** The DPIA must also evaluate risks to the data subjects and the measures envisaged to address the risks. In other words, can the SP effectively treat risks to personal data? These include safeguards and security measures designed to protect personal data and having in place adequate controls such as access control, anonymisation, among others. Additionally, the HBP partners must have tools in place to demonstrate compliance.
- 4) **Validation of the DPIA:** Following the assessment of the points above, HBP partners must make a determination of whether the controls in place are sufficient to protect the data subjects. If not, the HBP partners must determine what improvements can be made or

controls that might be added. In addition, the HBP partners will need to determine if it is necessary to consult with data protection authorities (evaluated below).

Taking the example of the MIP, the principles described above are displayed in the CNIL software as follows.



Based on the outcome of the DPIA, including the seriousness of the risks and the likelihood of occurrence, a decision must be made on the processing activity.



In the example above, the DPIA determined that the risk seriousness is negligible, and that the risk likelihood is negligible.

## 4. Data Anonymisation

As provided above, the GDPR only applies to [personal data](#) or information concerning an identified or identifiable natural person. If data are anonymised, it is no longer considered to be personal and is thus outside the scope of GDPR application. In other words, if data in an SP are anonymous, the GDPR does not apply and the data can be processed for research purposes without the restrictions of data protection law.

However, given the difficulty in creating truly anonymous data, the bar for anonymisation has been set extremely high under EU data protection law. To determine whether a person is identifiable, SP partners must consider “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 make this determination, SP partners must consider 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.” In making this determination, SP partners must consider the robustness of the anonymisation techniques they apply and the potential for failure of those techniques.

The main anonymisation techniques applied in data protection law are randomisation and generalisation. Regardless of the technique applied (e.g. addition, permutation, differential



privacy, aggregation, k-anonymity, l-diversity, t-closeness, etc.), three main questions should be considered:

- 1) Is it still possible to single out an individual?
- 2) Is it still possible to link records relating to an individual?
- 3) Can information be inferred concerning an individual?

The table below shows the strengths and weaknesses of some of most common anonymisation techniques. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques.

	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenisation	Yes	Yes	May not

### [Strengths and weaknesses of different anonymisation techniques \(WP216\)](#)

Although there is no prescriptive standard for in the EU, in one of the few areas of guidance, the Working Party 29 states that anonymisation requires “irreversibility preventing identification of the data subject” taking into account all the means “reasonably likely to be used” for identification. Although this ‘zero risk’ approach has also been criticised, it is the position taken by regulators.

#### **Anonymisation and Pseudonymisation in the HBP:**

**Pseudonymisation:** In some areas of the HBP, there has been confusion regarding the differences between pseudonymised data and anonymised data. Pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a dataset with the original identity of a data subject. Because the data subject is still identifiable with the use, inclusion, or cross-referencing of additional information, the data subject is considered identifiable and the GDPR remains applicable.

If HBP human data require re-identification at some point, the data are not anonymised for purposes of the GDPR. The GDPR will remain applicable. Personal data that have been pseudonymised data, including encrypted data, are provided with certain advantages under the GDPR such as data breach reporting. Whenever possible, personal data in HBP data should be pseudonymised. However, the GDPR still applies to pseudonymised data because the data can be attributed to a natural person by the use of additional information such as a decryption key.

**Anonymisation:** The optimal solution used by an SP for anonymisation must be decided on a case-by-case basis, possibly by using a combination of different techniques described above. Generally, these will include:

- 1) **Randomisation:** Remove strong link between the data and the individual. Common techniques include permutation and Differential Privacy.
- 2) **Generalisation:** Aggregating or generalising data (l-diversity, t-closeness, etc.).

SPs must account for the following risks:

**Singling out**—isolate some or all records which identify an individual in the dataset;

**Linkability**—ability to link, at least, two records concerning the same data subject or a group of data subjects



**Inference**—the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes

SPs that rely upon anonymisation must evaluate its robustness. Advancements in technology, such as ‘big data’ and associated analytical techniques, complicate this assessment.<sup>94</sup> The reality is that data that are truly anonymous in 2018 may be identifiable in 2028 given the likelihood of increased computing power and/or the ability to combine multiple datasets. Additionally, if data is provided to a third party in an anonymous format, and the third party combines the data or processes it in a way that allows for identification, then EU data protection law will again apply because the data will no longer be anonymous.<sup>95</sup> In other words, the status of anonymous data is not static. This should be done as part of the DPIA or other review.



## HBP Medical Informatics Platform (MIP) Example

**MIP Local:** Data stored on the MIP local will be pseudonymised using strong encryption and hashing, among other techniques. Data stored on the MIP local (pseudonymised data) are attributable to a natural person by the use of additional information, which is securely stored using both organisational and technical security measures.

**MIP Federated:** Data at the MIP federated level will be anonymised. The MIP federated applies both randomisation and generalisation techniques. MIP federated users cannot single out data subjects by identifying a patient within the MIP data set. Because of the generalisation/aggregation safeguards applied, it is not possible for users to isolate a link to the records to a single data subject or group of data subjects. Queries and available results are closely controlled. Therefore, it is not possible to infer or deduce values that might be used to identify a specific data subject.

The following points are examples taken from the MIP de-identification strategy. Further explanation is also available in ‘D8.6.1 (D48.1 D14) SP8 Medical Informatics Platform - Architecture and Deployment Plan’ on pages 22-27, available [here](#).<sup>96</sup>

Points in the strategy include:

- Information that is not needed for research purposes is removed;
- Identifiers are pseudonymised (replaced with a generated pseudo-identifier (hash));
- The link between the original identifier and the pseudo-identifier is stored separately from the information in dedicated database;
- All other identifiers present in the original data (visit id, etc.) will also be pseudonymised;
- The birth dates will be reduced to the year;
- All other dates will be reduced to the month: this level of detail is required for longitudinal studies;
- Patient names, addresses and similar personal information should not appear in data provided for the Platform and if they do, they are removed at the de-identification level;
- Specific de-identification rules can be defined for other fields based on the MIP or the partner's requirements;

<sup>94</sup> WP29 216 (2014) 9.

<sup>95</sup> WP29 216 (2014) 10.

<sup>96</sup> [https://sos-ch-dk-2.exo.io/public-website-production/filer\\_public/15/f1/15f199f8-4c69-4ac1-ae84-0dd6aa5ca7f0/d861\\_d481\\_d48\\_sga1\\_m6\\_accepted\\_180709.pdf](https://sos-ch-dk-2.exo.io/public-website-production/filer_public/15/f1/15f199f8-4c69-4ac1-ae84-0dd6aa5ca7f0/d861_d481_d48_sga1_m6_accepted_180709.pdf)

- A unique and well-defined pattern for dates is followed, such as dd/mm/yyyy (any pattern is acceptable). Date field must not contain anything else (no text, annotations, incomplete dates, etc.)
- Only one type of data per column (either numerical, date, text, etc.)

## 5. International data Transfers

Although EU legislators acknowledge that transferring data to third countries is often necessary, such transfers also have the potential to undermine the protections afforded to European citizens.<sup>97</sup> To address this balance, the GDPR restricts the transfers or ‘exports’ of personal data outside of the EEA to third countries that do not ensure an “...an adequate level of protection”.<sup>98</sup> Although left undefined in the GDPR, transfers generally concentrate on the physical location of infrastructure and any movement to or from those points. In some cases, data are transferred to third countries as part of research activities. In others, such transfers are inadvertent. For example, HBP partners using cloud storage will often transfer data to the US.

The GDPR does not radically change the status quo of the Directive regarding data transfers.<sup>99</sup> If an SP partner was compliant with the Directive, their means of transfer is also likely compliant with the GDPR. General rules regarding international data transfers are as follows:

- 1) Data transfers within the EU/EEA are deemed to have an ‘adequate level of protection’ and are permitted without limitation.<sup>100</sup>
- 2) Data may also be transferred to non-EU countries with an ‘adequate level of protection’ without limitation.<sup>101</sup>
- 3) Data may also be transferred if adequate safeguards are in place (e.g. Standard Contractual Clauses).
- 4) Data may also be transferred using a derogation from the main rule in some limited circumstances (e.g. consent).

Absent adequacy in (1) and (2) or the exceptions listed in (2) (3) (4), the GDPR prohibits data transfers to third countries. Adequate safeguards are evaluated further below.

### 5.1 Privacy Shield

The US does not offer an adequate level of data protection. As a result, personal data in SPs cannot flow freely from the EU to the US. Until 2015, the EC accommodated transatlantic data transfers through the Safe Harbour Framework. However, the Safe Harbour Framework met its end in the landmark case of *Maximillian Schrems v Data Protection Commissioner*. Following the decision in *Schrems*, the EU and US developed the Privacy Shield Framework.

SP partners can use the privacy shield framework to transfer data to the EU. A registry of participating/certified companies is available [here](https://www.privacyshield.gov/list).<sup>102</sup>

<sup>97</sup> GDPR Art 44. Expanded further in Recital 101.

<sup>98</sup> GDPR Art 45(1) and Recital 103.

<sup>99</sup> However, it will ease notification/authorisation requirements currently required by DPAs in some EU member states. See GDPR 45(1).

<sup>100</sup> GDPR Art 1(3).

<sup>101</sup> The EC recognises Andorra, Argentina, Canada (limited to commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework), available at [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en).

<sup>102</sup> <https://www.privacyshield.gov/list>.

## 5.2 Appropriate safeguards

Even if the third country does not provide an adequate level of protection, transfers of personal data are still possible. However, the SP making the transfer will have to apply “appropriate safeguards” to guarantee that the fundamental rights of data subjects are protected.<sup>103</sup> These generally include binding corporate rules (BCRs), ad hoc, or standard contractual clauses (SCCs) as adopted by the EC.<sup>104</sup> The GDPR also provides the possibility for international transfers based on codes of conduct and other certification schemes. However, no certification schemes or codes of conduct for international transfers have been approved.

### 5.2.1 Standard contractual clauses

If a third country does not offer an adequate level of protection, data transfers can be accomplished using contracts.<sup>105</sup> That is, the parties to the transfer can contractually commit to provide an adequate level of protection. Although contracts can be tailored and adopted on an ad hoc basis for individual approval, SCCs (Standard Contractual Clauses) drafted by the EC are also available. The EC’s SCCs are a popular tool for international data transfers to third countries.<sup>106</sup> The EC has adopted three sets of SCCs: two focus on controller-to-controller transfers and the third focuses on controller-to-processor transfers.

The SCCs drafted by the EC essentially function as standards. For instance, altering or partially adopting SCCs invalidates the ‘adequacy’ protection they provide.<sup>107</sup> Although SCCs can be combined or presented as part of a larger contract, the SCC terms cannot be altered. As a result, SCCs provide little flexibility. SP partners relying on SCCs should adopt unmodified standard terms when possible. For SP partners that have SCCs adopted under the Directive remain valid under the GDPR.<sup>108</sup>

### 5.2.2 Binding corporate rules

In addition to SCCs, BCRs (Binding Corporate Rules) provide a means to transfer data within a corporate group. Although certain actors in the group may be located in third countries which lack adequacy, the group as a whole offers an adequate level of protection. Unlike the Directive, the GDPR specifically recognises BCRs.<sup>109</sup>

For SP partners, using providers that have BCRs is also an option.

## 5.3 Derogations

The GDPR also allows for the possibility of international transfers of data to third countries lacking both ‘adequacy’ and the ‘appropriate safeguards’ evaluated above.<sup>110</sup> In certain limited situations, data can be transferred to third countries based on explicit consent, the performance or conclusion of a contract, or when the transfer “is necessary for important reasons of public

---

<sup>103</sup> GDPR Art 46(1). See further GDPR Recital 108. At the time of writing, no certification schemes or codes of conduct approved for international transfers have been completed.

<sup>104</sup> GDPR Art 46 (2) (a-f) and 46 (3) (a-b). For further details on binding corporate rules, see GDPR Art 47.

<sup>105</sup> GDPR Art 46 (3)(a).

<sup>106</sup> GDPR Art 46(2).

<sup>107</sup> WP29 196 (2012) 18-9.

<sup>108</sup> GDPR Art 46 (5).

<sup>109</sup> GDPR Art 47.

<sup>110</sup> GDPR Art 49

interest”, among others.<sup>111</sup> However, such transfers have limited applicability and should only take place when other means are unavailable and the transfers are not reoccurring.<sup>112</sup>

In short, although the exception is available, SP partners cannot build their data sharing plans around these derogations. The derogations do not provide long-term solutions.<sup>113</sup>

## International Data transfers in the HBP

- 1) Data transfers within the EU/EEA→ No restriction
- 2) Data transfers to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay→ No restriction
- 3) Data Transfers with appropriate safeguards to guarantee that the fundamental rights of data subjects are protected. These tools include:
  - Standard Contractual Clauses (SCCs)
  - Binding corporate rules (BCRs). Generally set up by a provider.
  - Privacy Shield
  - Derogations (limited)



International data transfers are one of the most complex aspects of EU data protection law. It is also an area with ongoing litigation challenging some of the means for transfer (i.e. Privacy Shield and SCCs). The DPO will monitor changes and provide updates.

<sup>111</sup> GDPR Art 49(1) (a-f).

<sup>112</sup> GDPR Art 49(1).

<sup>113</sup> The European Data Protection Board (EDPB) adopted Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Available at [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_2\\_2018\\_derogations\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf)

## Part II: Data Contribution and Model Organism Data (Animal Data)

The policies described in this section were developed with particular attention to the work of the Neuroinformatics Platform (NIP, SP5), but they apply to all data in the HBP. In particular, this section focuses on model organism data (animal data).

The HBP adopts the policies set out in this section 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](#) and implementation-level policies described in the [Research Data Alliance \(RDA\) Practical Policy](#) 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 in this area.

## 6. Model Organism Data

### 6.1 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.

## 6.2 HBP storage and Knowledge Graph

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

Knowledge Graph 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 and outlined in the Data Registration Process (below).

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.

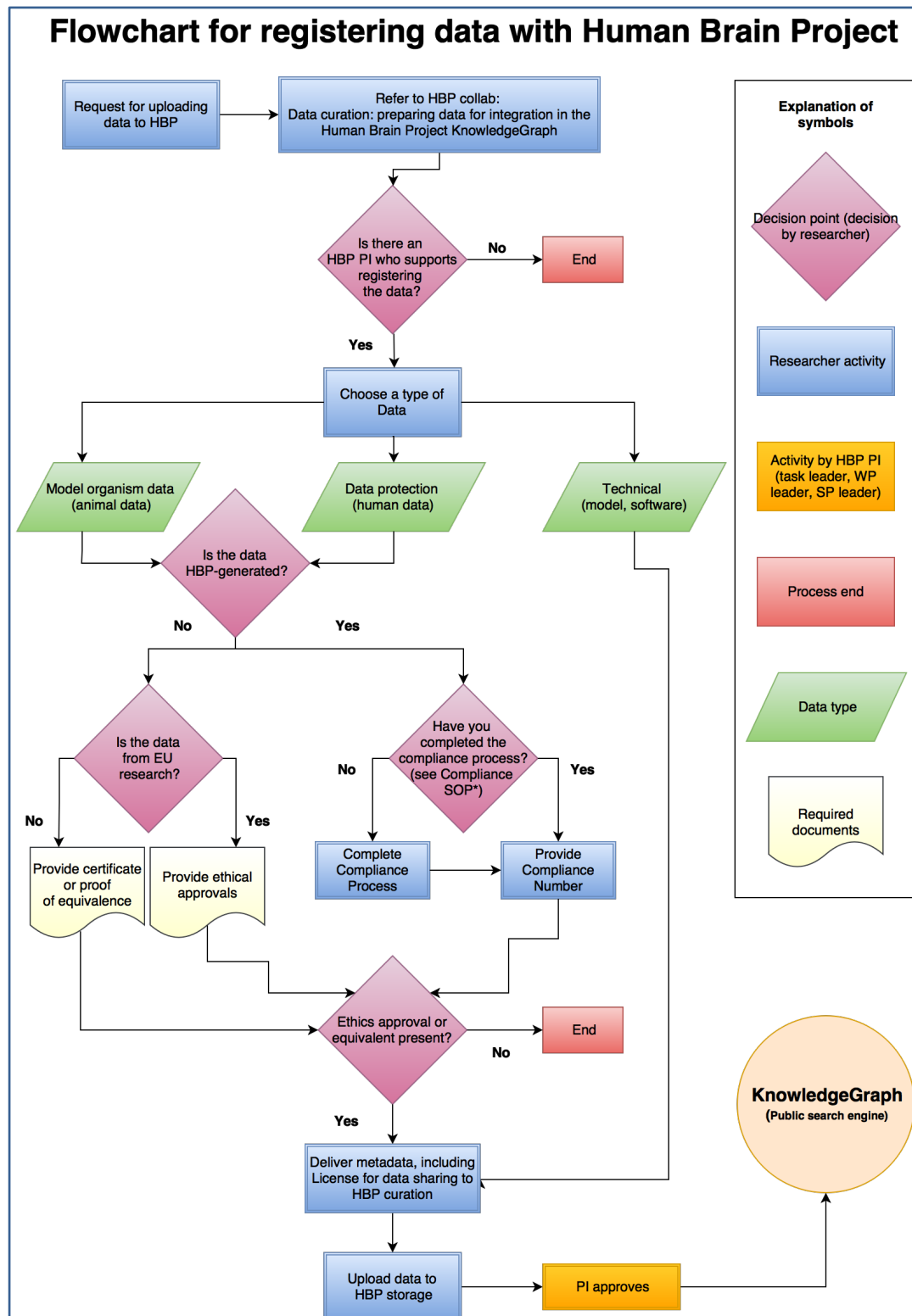
Metadata for data stored in HBP storage will be stored in the HBP Knowledge Graph. All metadata in the HBP Knowledge Graph are openly searchable.

## 6.3 Data Registration

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

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





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 serialised in a format that is registered in a data format index.
  - To ensure that data remain accessible after they have initially been made accessible, HBP maintains a list of serialisation 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.

## 6.4 Ethics compliance (animal data)

- For data sourced from animal studies commissioned by/financed through the HBP, the Data Contributor confirms that the data were collected in research that complied with:
  - Ethical principles as outlined by the [Horizon 2020 Ethics Self-Assessment](#)<sup>114</sup>
  - Applicable international, EU and national law (in particular, EU Directive 2010/63/EU)<sup>115</sup>.
  - 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 are sourced from facilities which have proven compliance with the US ILAR Guide for the Care and Use of Laboratory Animals<sup>116</sup> 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

<sup>114</sup> [http://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-msca-itn-2015/1620147-h2020-guidance\\_ethics\\_self\\_assess\\_en.pdf](http://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-msca-itn-2015/1620147-h2020-guidance_ethics_self_assess_en.pdf)

<sup>115</sup> 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).

<sup>116</sup> <https://grants.nih.gov/grants/olaw/Guide-for-the-Care-and-use-of-laboratory-animals.pdf>, accessed 23.08.2016

Accreditation of Laboratory Animal Care) accreditation, or by a publication in an international tier 1 peer-reviewed journal that endorses the ARRIVE guidelines.<sup>117</sup>

- In cases where the above cannot 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.
- 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<sup>118</sup>.

## 6.5 Data Licensing

This section addresses HBP policy for data licensing. While software can be considered data, this section does not relate to software licensing policies.

All data registered with the HBP that are protected by copyright 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<sup>119</sup>. 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:

<sup>117</sup> <https://www.nc3rs.org.uk/arrive-animal-research-reporting-vivo-experiments#journals>, accessed 17.08.2016

<sup>118</sup> [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](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)

<sup>119</sup> <https://creativecommons.org/choose/>

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


## DPM Inventories and Worksheets

The following section is reserved for templates/worksheets.

### Inventory I: Controller/SP Documentation Worksheet

#### HBP GDPR Documentation Worksheet: Data Controller

The inventory below is a tool of SPs to evaluate the data they have in their project as personal.

 <p>Human Brain Project</p>
<p><b>HBP GDPR Article 30 Documentation Worksheet: <u>Data Controller</u></b></p> <p>Initial survey to gather information for <a href="#">documentation</a> requirements. Fill in the following categories. For further explanation, see the DPM.</p>
<p><b>SP partner (Name and role in HBP)</b></p>
<p>Name/Role of individual completing:</p> <p>Name of Organisation:</p> <p>Specific Department:</p>
<p>Local Data Protection Officer (if applicable):</p>
<p>Data protection contact person (if different from the DPO):</p>
<p><b>Joint Controller (if applicable):</b></p>
<p>Name of Organisation:</p> <p>Specific Department:</p> <p>Contact Person:</p> <p>Contact Information:</p>

Local Data Protection Officer (if applicable):

Data protection contact person:

**Data Processor(s):**

Contact Person:

Contact Information:

Name of Organisation:

Location(s) of processor(s):

If a cloud service provider, provide name and a contract:

Local Data Protection Officer (if applicable):

Data protection contact person:

Please attach a copy of that agreement if possible

**Short Description of Solution/System(s):**

**Description of the [Purpose](#) of Processing**

Short description (e.g. medical research):

**Personal Data Inventory (Categories):**

Who do you hold data about (e.g. patients, survey participants, external researchers)?





What data do you hold about them (e.g. contact details, survey results, medical records, etc.)?

**Data Subjects:** list the primary categories of data subjects including patients, employees, researchers etc.

**Personal Data:** list all types of [personal data](#) processed in the system including:

(1) General personal data (e.g. names, account data).

(2) Sensitive personal data (e.g. medical reports, MRIs, or other genetic data).

**Source of the Personal Data** (e.g. patient, hospital, partner university, external research project, public domain etc.).

#### International Transfers of Personal Data/Data Flow

(1) Does the SP partner transfer data outside of the EU/EEA? If so, please list countries:

(2) If the SP partner transfers data outside of the EU/EEA, what safeguards are in place (e.g. SCCs, BCRs, Privacy Shield, etc.).

(3) Does the SP partner receive data from a country or countries outside of the EU/EEA? If so, please list countries:

#### Data Retention and Erasure Policy

How long do you store the personal data you collect? Do you have a policy for erasure or deletion of data?

## Processing Operations

Describe the type of processing that takes place. For example, storage, anonymisation or de-identification processes creation of statistics etc.

## Legal Basis for the Processing of Personal Data

Describe the [legal basis](#) used for the data processing (e.g. consent, performance of a contract, compliance with a legal obligation, etc.).

If the personal data processed in the SP partner uses more than one legal basis, specify the basis as applied to the personal data.

## Legal Basis for Processing of Sensitive Personal Data

Describe the legal basis used for the data processing (e.g. explicit consent).

## General description of technical and organisational security measures (e.g. encrypted storage, access controls etc.)

- Have your SP partners had a Privacy Impact Assessment (PIA) or a Data Protection Impact Assessment? If so, please send a copy of the impact assessment to the DPO.



- Can you document that you have followed ‘best practices’ regarding data security? In particular, have you obtained certifications, audits (accredited or otherwise).

## Data Protection by Design and by Default

Have you implemented the principles of data protection by design and default?

Briefly describe any processes/tools you apply including data minimisation, de-identification (e.g. pseudonymisation) or anonymisation.

## Data Processing Agreements

Controller:

- Do you have a *data processing agreement* with processors?
- Name and location of processors
- Please attach a copy of that agreement if possible

Processor:

- Name of controller
- Do you use subcontractors or sub processors?
- Do you have a process in place for obtaining controller consent for adding new processors?
- Name and locations of processors

## General

- Do you have access to legal counsel for data protection related queries?
- Do you have a GDPR readiness program? If so, what is the completion status?
- Please attach copies of relevant documents including PIAs, DPIAs, internal analysis from GDPR projects

## **Inventory II: DPIA Template**

Worksheet/inventory draft under revision.

## **Inventory III: Data Protection by Design and Data Protection by Default**

Worksheet/inventory draft under revision.

## **Inventory IV: General Security of Personal Data Inventory**

Worksheet/inventory draft under revision. Overview provided [above](#).