Title:	Terms of Reference: HBP SGA2 Data Governance Working Group Data Audit Committees
Partner Responsible:	DMU
SP / WP / Task Involved:	All SPs

Authors:	T. Fothergill, K. McGillivray
Contributors:	All members of the Data Governance Working Group
Editor:	T. Fothergill

Document Approval Status

Date	Comments
00/05/2018	Initial draft (Tyr)
20/11/2018	Updated draft and suggested TOR content and procedure (Kevin)
15/12/2018	Review by Tade Spranger and Josep Domingo-Ferrer of the EAB
01/02/2019	Revisions in response to the EAB and internal DGWG reviewers (Tyr)
11/02/2019	Approval by the SIB
10/04/2019	Revisions requested by the DIR and made by Tyr Fothergill of the DGWG
10/04/2019	Approval by the DIR
18/04/2019	Finalisation by DGWG

1. Purpose

The DGWG is tasked with establishing appropriate data and digital information governance practices for the HBP. In addition to establishing policies and procedures, the DGWG also assists with implementation of data governance objectives across the project. Particularly, the DGWG creates policies to ensure that the HBP's strategies and objectives regarding data security and data protection, as decided by the governing bodies of the HBP in response to ethical and regulatory requirements, are reflected throughout the project. These policies are vital for successful scientific research in the legal context of the General Data Protection Regulation (GDPR)[1], and are part of demonstrating socially-responsible practices. Policies developed by the DGWG are intended for implementation at the level of the HBP team operating within their local institutional context. The following 'Data Governance Audit Committee Terms of Reference' sets the parameters for the DGWG to arrange collaborative, voluntary audits and compliance checks of specific systems or aspects within the project.

The purpose of an audit is to determine whether a specific data-related system, service, or aspect of the HBP is operationally aligned with the GDPR and relevant HBP-specific policies and procedures as implemented by the HBP group involved, which may be cross-institutional

[1] See GDPR Recital (33) and Article 89(1)

and complex depending upon the focus of the audit. In addition to providing the project with an opportunity to address deficiencies internally, audits provide an opportunity to raise awareness of data protection requirements, potential data-related ethical issues, security needs, and cybersecurity obligations across the HBP. They are also intended to serve as a preparatory tool for interactions with Data Protection Authorities. Furthermore, conducting internal audits on a voluntary basis openly demonstrates an aspect of the HBP's commitment to data protection, accountability, and the rights of data subjects beyond conducting Data Protection Impact Assessments. Examples of best practice will also be revealed through these audits, and may be shared with other HBP groups to enhance project-wide performance. Finally, such audits also provide a means of showing that HBP policies have been implemented in context-appropriate ways. The relevant HBP policies include those set forth in the Data Policy Manual (DPM) and the Data Management Plan (DMP). Should the audit reveal that the DPM and DMP have not been adequately implemented, the process provides the relevant group(s) within the project with the opportunity for dialogue with the DGWG or other bodies to support correction or re-alignment with HBP policy.

2. Process

In Section 3.2 of Part B of the SGA2 GA[2], the HBP Data Governance Working Group (DGWG) was allocated responsibility for creating ad hoc Data Governance Audit Committees and the process of constituting these. The purpose of these Committees is to conduct ad hoc compliance audits of HBP policies contained in the Data Policy Manual and the Data Management Plan.

2.1 Activation and Requirements of an Audit

Data Governance audits may be triggered by a request to the standing data governance audit committee (from an SP leader, a member of the DGWG, or the DPO, for example). Such a request may be made in response to a structural change or event, including infrastructural or administrative alterations, a failure to provide required documentation (e.g. a certificate or approval), or an order from a Data Protection Authority. The activation of an audit requires submission of a request to the standing data governance audit committee with the following information:

- Specific designation of the HBP task, system, service, or data type to be audited;
- The individuals, groups, teams, and/or SP(s) responsible;
- The reason(s) for requesting a Data Governance Audit;

[2] Appendix 1: HBP SGA2 Use Cases, SGA2-SP12-UC003

- Any specific concerns or other pertinent information which the DGWG may not be aware of, i.e. local or institutional timing issues and deadlines, personnel absences or changes, local Data Protection Authority involvement, etc.

To conduct an audit, the DGWG data governance audit committee will rely primarily on a cooperative and open dialogue with the HBP partner(s) under audit. Although data audits will generally take place at the level of the HBP group involved in the relevant system or aspect, more complex situations may involve several partners or task leaders from one or more SP and a multi-scalar or distributed approach may be necessary.

Audits will primarily require an explanation of how the partner has implemented the policies outlined in the DPM and the DMP within their HBP task or institution. Partners should also provide an explanation of their training and awareness processes regarding these documents. Additionally, partners will generally be asked to provide an explanation of data security practices in place, including asset management, access control, physical security, cybersecurity, operations security, communications security, and incident management. The audit committee will generally require evidence or documentation from the partner, including evidence in the form of records of data processing activities, privacy policies, risk registries, and internal governance structures and related workflows or processes. Other relevant information, such as external audits or certifications, should also be provided to the audit committee.

The partner should also be prepared to identify and make available key people that have been involved in and have the expertise to answer questions regarding data protection, data security, and data governance as they pertain to the task, system, or service under audit.

The audits conducted by Data Governance Audit Committees may take place no more often than yearly for each data type, system, task, or service, though this may vary depending upon the reasons for audit and the availability of resources to undertake audits. The scope of each audit will be limited to specific services, tasks, data types, systems, or workflows. As these will require subject-specific expertise, the specific structure and format of the audit will be determined by the membership of each Audit Committee (see below).

3. Audit Committee Membership and Selection

The Data Governance Working Group will discuss and nominate candidates for appointment to Data Governance Audit Committees after the purpose of the Data Governance Audit Committee has been designated as part of the audit triggering process. Membership of these Audit Committees shall be determined by the potential appointee's experience and expertise

working with the data types and infrastructure used by the group under audit, and will include individuals with knowledge of local processes.

To support and maintain effective internal control of the Data Governance Audit Committee formation process, the DGWG will create a standing data governance audit committee comprised of members of the DGWG which will be responsible for: (1) receiving requests for the constitution of Data Governance Audit Committees for carrying out data governance audits of HBP tasks, systems, or services; and either (2) suggesting and appointing auditors for the specific circumstances appropriate to the system under audit and its context; or (3) conducting audits in more general cases; as well as (4) receiving the combined audit report generated by nominated Data Governance Audit Committees and (5) supporting post-audit follow-up actions.

In determining appointments, the DGWG standing data governance audit committee will consider aspects such as familiarity with routines and processes of the subproject, task, or system under audit, technical and operational expertise, and/or overall knowledge of the relevant subproject and/or institutions. Audit Committees must include individuals with technological expertise appropriate to the system under audit, in particular because the GDPR requires some assessment of risk. The expertise and experience of local team members with direct knowledge of the systems, services, and data types in use is therefore critical for the success of the Data Audit process.

In some instances, a conflict of interest may arise wherein a member of the DGWG is not sufficiently impartial to serve on a Data Governance Audit Committee in an unbiased fashion due to their working proximity to the system, institution, or task under audit. In such a case, the member should disclose their conflict of interest as soon as the data audit has been triggered and not participate in the respective Data Governance Audit Committee for that particular audit. Should a potential conflict of interest arise and not be disclosed, it is the responsibility of the Ethics Director and DGWG Chairs to notify the member that their participation in that specific audit will not take place.

If the DGWG standing data governance audit committee is unable to find qualified auditors within the HBP, the committee may also suggest that an external auditor conduct the examination or become part of the Data Governance Audit Committee. External auditors should be selected based on the same characteristics (i.e., their overall expertise and impartiality) as internal project auditors. Payment of external auditors, if necessary, should be at the European Commission Expert Reviewer rate of €450 for each full day worked. If appropriate, the DGWG may also consult the EAB on the subject of potential auditors and/or auditor suitability.

3.1 Duration of membership

Standing data governance audit committee members will serve in that capacity until they choose to withdraw from the role, they are no longer affiliated with the Human Brain Project, or a conflict of interest arises. Data Governance Audit Committee members will serve as part of that Committee only for the duration of the Audit process, including preparation, assessment, reporting of results, and any actions arising from the audit result.

4. Audit Committee Process

Once the standing data governance audit committee is presented with a request for an audit, they will consider the requirements of the situation and appoint the Data Governance Audit Committee membership in cooperation with SP members or those most familiar with the system or service under audit. The Ethics Director will make the presence of the committees known to the DIR and the Stakeholder Board, and the Stakeholder Board will approve the Data Governance Audit Committees prior to the audit taking place.

Once appointed, the membership of the Data Governance Audit Committee must:

- Notify the SB and SCSB of their presence and the scope of the audit;
- Meet to review and assess the situation of the audit subject;
- Request assistance from other individuals, groups, and/or SPs when needed for the audit;
- Verify required ethical approvals and request additional documents as necessary to perform the audit; and
- Remain available for requests for clarification after the audit is complete.

5. Scope of audit

The scope of Data Policy audits will be determined in part by the nature and level of the request for audit, which can originate from multiple sources (e.g. the DPO is carrying out a DPIA, a task leader is working on a platform or service and wishes to assess their team's compliance with HBP Data Policies, an SP leader with responsibility for a new CDP wants to ensure consistency, a data breach needs to be assessed, etc.).

Generally, the material scope of the audit will include an evaluation of data protection governance and accountability. This will be primarily assessed based on the implementation of the DPM, DMP, and additional HBP routines and procedures as appropriate (e.g. privacy by design in the HBP) as well as any relevant SP or Task-specific policies covering data use. This assessment will evaluate whether the partner can demonstrate that they have adequate

policies in place. For instance, if the partner 'produces data,' they must demonstrate that they have a legal basis for data processing, adequate records of processing activities, data retention schedules, the ability to demonstrate consent, among other procedures. If the partner shares data, this means being able to demonstrate they have data processing agreements/addendums and other protocols in place. This information will be primarily self-reported.

The Data Governance Audit Committee may also consider whether the partner reported their data-related risks in the project-wide risk register, has given an accurate assessment of these risks in the one-pager, and reported their data processing operations to the DPO. In addition to HBP specific obligations, weight will also be placed on general risk management and evaluation, security practices, records management, consideration for data-related ethical issues, and other relevant elements of the partner's processing activities such as a data retention schedule or institutional data security policy documentation.

Relevant documentation that falls within the scope of this assessment includes copies of contracts and data sharing agreements, data protection impact assessments (DPIAs), audit and vulnerability testing reports, incident logs, asset registers, data destruction records and certificates, among others.

6. Reporting of Results

Upon completion of the requisite audit, each Data Governance Audit Committee will create a combined audit report of their findings. The report will include the committee's evaluation and recommendations, along with any relevant exchanges of information and communications and a high-level summary. In particular, the report will highlight areas of non-conformance with HBP policies and other areas where partner actions have the potential to create project risks, as well as cases in which best practice is evident. Where possible, the Audit Committee report should also include prioritised recommendations to mitigate risks. These recommendations will apply the following structure, and in certain high-risk situations, may include a follow-up audit within a timeframe as appropriate to the level of risk.

Urgent Priority Recommendations: The partner or service creates clear and immediate risks to the project in the areas of data protection and/or data security. The risks must be addressed immediately.
High Priority Recommendations: The partner or service creates risks that should be addressed quickly in order to mitigate risks to the project in the areas of data protection and/or data security.

Medium Priority Recommendations: Areas where the severity of the risk is medium to high but the likelihood of occurrence is low. In medium priority recommendations, the Audit Committee may recommend mitigating measures or a timeline for compliance.
Low Priority recommendations: Areas where the severity of the risk is low and the likelihood of occurrence is also low.

The partner will have three weeks (21 days) to respond to the audit report before it is finalised by the Data Governance Audit Committee. In complex cases, partners may request an extension of two additional weeks. If the Data Governance Audit Committee determines that a partner has dealt with a risk effectively, the report should also make note of the approach and consider its relevance on a project-wide basis. Instances of best practice may also be summarised and disseminated across the project.

The report of the Data Governance Audit Committee will be primarily provided to the DIR as decision-makers. They will also report their findings to the DGWG, and the highest levels of HBP governance, including the SIB, SB, and SCSB. It will also be made available to the group responsible for the audited system, service, or task. The high-level summary portion of the report will be made available internally to other HBP partners.

Should a situation which presents data governance-related risks arise repeatedly within the HBP, the standing data governance audit committee will prepare a summary report on the issue(s) for the DIR and other HBP governance bodies and, if possible, outline potential recommendations for methods of preventing future re-occurrences of the issue.

6.1 Follow-up and corrective actions

Depending on the results of the audit, the partner may be asked to take corrective action. Generally, this will require a short follow-up report from the group responsible for the audited task, service, or system which outlines the steps they have taken to meet the corrective action requirements. This report should be developed on a timeline appropriate to the extent and severity of measures which are necessary to implement. Follow-up reports in Data Protection contexts are generally expected to be delivered within 6-12 months of the initial audit[3]. However, the situational level of urgency and legal implications will determine the immediacy of reporting and associated actions. For example, should a personal data breach be detected during the course of an audit, the timeline and actions described in Article 33[4]

[3] For example, as described in section 3 of the ico guidance on data protection audits https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf

[4] https://gdpr-info.eu/art-33-gdpr/

should be followed in reporting (i.e. within 72 hours). In exceptional cases, the Audit Committee may request or require an independent or third-party audit.

6.2 In case of audit failure

Should the task, system, service, etc. being audited fail the assessment of HBP Data Policy compliance by the Data Governance Audit Committee, various actions may be taken by the Committee, including (but not limited to):

- Contacting the relevant data protection authority and/or data subjects
- Removal or prohibition of access to HBP Services and Platforms (in consultation with the DPO and HBP System Administrators);
- Local institutions may be informed of possible research misconduct by the Ethics Manager, and/or be required to make a public statement regarding ethical aspects of the research (or researcher) involved in the audit failure; and
- If the audit failure involved incorrect processing of personal data, the DIR will be notified.

7. Disbanding of Audit Committees

The standing data governance audit committee will remain available on an *ad hoc* basis for the purposes of receiving requests for creating audit-specific Data Governance Audit Committees and selecting the membership of these Committees. Each Data Governance Audit Committee will be disbanded at the point at which final reporting has been completed, with long-term follow-up of corrective or other measures undertaken by members of the group responsible for the audited system, service, or task with support from the standing data governance audit committee (as long as the necessary expertise to do so exists). For this reason, individual members of Audit Committees should agree to remain available for requests for clarification.

7.1 Data Retention

Personal data collected for audit purposes will be returned or deleted when the purpose of the audit has been completed. In cases where the HBP has an obligation to retain such data for a longer period, audit data will be stored securely and in compliance with the relevant regulatory framework (the GDPR as well as any local or institutional requirements).

8. Approval and Revision

After approval by the Data Governance Working Group, these terms of reference will be submitted to the SIB and then the DIR for approval. Once approved, this document will be regularly reviewed by the Data Governance Working Group and amended when significant changes are required.