Plan International UK

Data Protection Accountability Statement

DOCUMENT CONTROL INFORMATION:

Title	Data Protection Accountability Statement
Author (Responsible)	Data Protection Officer
Owner (Accountable)	Chief Operating Officer
Directorate	Operations
Contact	Head of IT
Version	1.2
Status	Approved
Reviewed by (Consulted)	Management Board
Approved by	Management Board
Date of Approval	09/09/2019
Applicable to (Informed)	All staff, all stakeholders (statement published on website)
Issued on	16 October 2019
Related policies & procedures	Data Protection Policy, Data Retention Policy, Unstructured Personal Data Standard, Information Security Policy, IT User Policy, Document Management Policy, Procurement Policy, Contract Signing Policy

DECISION-MAKING:

Decision	Accountable	Responsible	Consulted	Informed
All matters concerning this statement	COO	Head of IT	Management Board, Data Group	All staff, all stakeholders (via website)

Data Protection Accountability at Plan International UK

As part of our compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR), Plan UK has reviewed how we demonstrate accountability for our data processing activities.

Plan UK is not a public authority and does not carry out large scale processing of special categories of data or data relating to criminal convictions and offences. However, our core activities do involve large scale regular processing of personal data and we have therefore voluntarily appointed a Data Protection Officer (DPO) in compliance with Article 37 of GDPR. In addition, we have also appointed a Senior Information Risk Officer (SIRO).

Our DPO plays a key role in ensuring our accountability but is not solely responsible.

Our SIRO champions Information Security at the highest levels of management.

Plan UK has an Information Security Document Management System, defined within our Information Security Policy. This is the suite of policies and procedures which enables us to embed cultural and systematic good practice, identify and manage our information risks, and monitor compliance. This includes specified roles such as the DPO and SIRO (see Appendices A and B for more detail).

Key roles:

Senior Information Risk Owner – Bill Cunningham, Chief Operating Officer (COO)
Data Protection Officer – Alan McMahon, Head of IT
Information Asset Owners – all Heads of Unit are responsible for ensuring that their unit is compliant with data legislation

Our SIRO and DPO are responsible for making sure that an appropriate level of organisational and technical measures are in place to manage personal data at Plan UK, including the provision of relevant policies, procedures, and training.

Our DPO is responsible for providing advice, monitoring compliance and carrying out key tasks such as responding to subject access requests, handling security incidents, and promoting good privacy/security practices.

IAOs (Heads of Unit) are responsible for making sure that the business processes and decision making in their unit are in line with GDPR requirements and good practice.

Organisational measures:

Our approach has ‘privacy by design and default’ at the forefront. We have an established Data Protection Impact Assessment process led by our DPO who is available to provide advice throughout the process. This process is linked to our procurement, supplier assessment and contract management processes, and training is available to staff/teams on request.

We have key accountability documentation including a record of our processing activities (ROPA), Information Security Policy, and Data Retention Policy. Our business processes require that data-related decisions are documented. Our data protection policy mandates that every data subject about whom we process personal data will be made aware of our privacy notice https://plan-uk.org/terms-conditions/privacy-notices/privacy-notice).

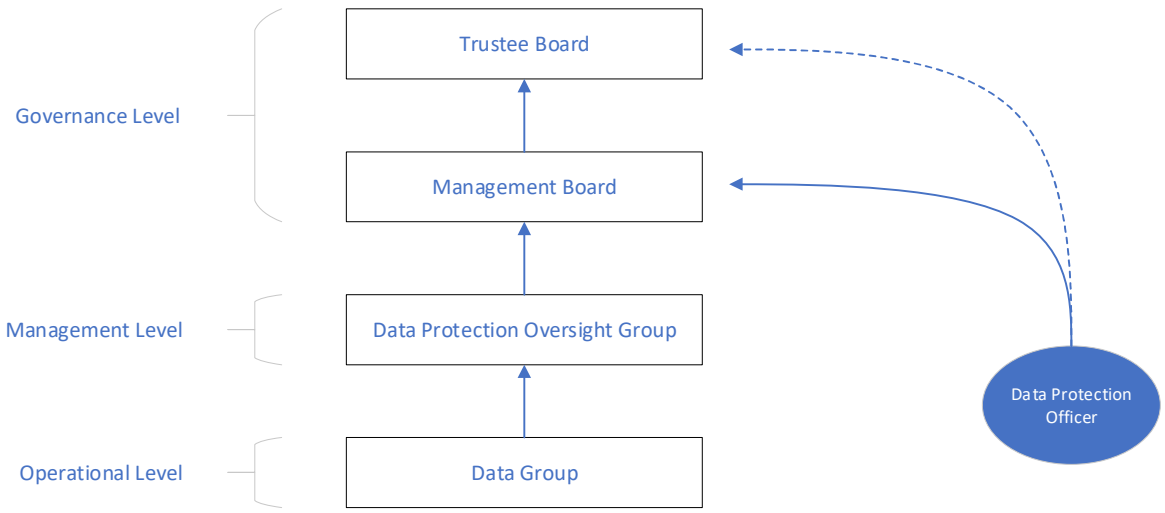
We maintain a data protection risk register that is reviewed quarterly by the DPO and SIRO. Required changes to any of our information security documentation is recorded in a central log pending updates to the relevant documentation.

Training in data protection and governance for new starters and existing staff is mandatory and ongoing. Where specific training needs are identified, we are committed to providing support.

We run quarterly 'Data Protection Oversight Group' (DPOG) meetings with CEO/Director level representatives in order to ensure an effective data protection compliance framework is in place and to ensure data protection risks and issues are dealt with at an appropriately senior level within Plan UK. See Appendix C for more detail.

We run quarterly 'Data Group' meetings with representatives from across the organisation in order to set priorities within our ongoing information compliance work and to improve awareness and local knowledge across the organisation, for example by providing tailored training to individual teams. See Appendix D for more detail.

The governance and reporting structure is summarised in the diagram below:



Our compliance with GDPR was most recently audited in 2018 by an external organisation. We maintain related externally-verified annual compliance measures such as Cyber Essentials and Payment Card Industry (PCI) compliance and also carry out annual penetration testing.

Our Data Protection Officer

Our Data Protection Officer is Alan McMahon. Alan is also the Head of IT. He has significant experience in data protection, holds a GDPR Practitioner certificate and is responsible for monitoring compliance at Plan UK. The DPO role has been defined and signed off by Plan UK's Management Board (Appendix A).

Independence

Our DPO is able to raise issues in the way and in the manner they see fit, without approval from their line manager (the SIRO, also COO) or others to do so. The DPO also has a dotted line reporting mechanism into a lead Data Protection trustee, and thus the Trustee Board. Our DPO is not penalised for performing their tasks or challenging the business.

Reporting to highest level of management

The DPO is accountable to Plan UK's Management Board, the most senior management body at Plan UK, consisting of the CEO and all directors of Plan UK (which therefore includes the SIRO).

The DPO provides an annual summary report to Management Board and the Trustee Board as well as reporting more frequently, including immediately, should the need arise (e.g. in the case of a data breach that was reportable to the Information Commissioner's Office).

The DPO is responsible for reporting risks or opportunities and recommending appropriate actions in relation to Plan UK's processing of personal information. Our DPO has regular contact with all members of our Senior Management Team (SMT). Our DPO has access to all of our information systems and access to all services and staff if they need input, information or support.

DPO tasks

The requirements of Article 39, as described by the ICO, are included in the DPO role profile, and have been formally approved by Management Board.

Our DPO's other tasks

We have appointed an internal employee as our DPO who has additional professional duties. As DPO and Head of IT, the tasks and focus of each role are reasonably complementary – and sitting in IT provides additional intelligence in terms of knowing about new systems or processes in development. The DPO is encouraged to raise any conflict of interest concerns with the Trustee Board.

Visibility

Our DPO's contact details are included within our privacy information and records of processing activities. We also include their contact details as part of the IT induction, which is completed by all staff. We have a dedicated email address and monitored inbox for data protection queries or complaints received internally or externally.

Our DPO is our contact with the Information Commissioner's Office in its capacity as UK supervisory authority.

Decision making

Where the advice of the DPO is not followed, this is documented.

If you have any queries, please email: dataprotectionofficer@plan-uk.org

ARCI

The ARCI matrix for roles and responsibilities for data protection is included below:

ARCI Key: A – Accountable; R – Responsible; C – Consulted; I – Informed

	Role or Function						
Activity	Senior Information Risk Officer	Data Protection Officer	Data Protection Oversight Group	Data Group	Management Board	Trustee Board	Info Asset Owners
Oversight and governance of Plan UK's data protection practices	R	R	C	I	C	A	I
Lead on organisational data protection legislation compliance	R	R	A	C	I	I	I
Ensure suitable Data Protection risk register in place	R	R	A	C	I	I	I
Put policies & procedures in place to ensure data protection compliance and mitigate risk	A	R	C	C	I	I	I
Prioritisation of ongoing data protection compliance work	C	A R	C	C	I	I	I
Review summary info of Data Privacy Impact Assessments and Data Breaches	C	R	A	I	I	I	I
Promote data protection awareness	C	A	I	R	I	I	I

APPENDIX A: Data Protection Officer (DPO) Role

ICO Guidelines

The DPO role, according to the Information Commissioner's Office (ICO), must:

- Report to the highest level of management
- Be sufficiently well resourced to perform their tasks
- Be able to operate independently, and not be penalised for performing DPO duties
- Be involved in a timely manner in all issues relating to the protection of personal data
- Not undertake other tasks or duties which result in a conflict of interests with their DPO duties

Plan UK Implementation

At Plan UK, our DPO is the Head of IT and is responsible for:

- Informing and advising the organisation, its employees and trustees about their obligations under GDPR
- Monitoring compliance with GDPR and related legislation and providing Management Board and Trustee Board with an annual summary report, as well as more frequent reporting, as required
- Being the external point of contact for data enquiries as per the general Privacy Notice on Plan UK's website and for any supervisory authorities, e.g. the ICO
- Overseeing the maintenance of Plan UK's data processing activities
- Leading on decisions relating to the requirement of Data Protection Impact Assessments (DPIAs) and their subsequent review
- Leading on the processing of Subject Access Requests
- Leading on the reporting and processing of any data breaches, including advising on action to prevent, or reduce likelihood of, recurrence
- Ensuring that effective data protection training for staff is in place
- Attending and reporting as required to the Data Protection Oversight Group
- Organising and chairing the Data Group meetings
- Presenting work proposals to the Data Protection Oversight Group and Data Group which ensure that the highest risk areas of data processing are regularly examined and any remedial actions carried out.

Approved by Management Board: September 2019

APPENDIX B: Senior Information Risk Officer (SIRO) Role

General Considerations

A SIRO is the member on the Management Board of an organisation with overall responsibility for the organisation's approach to managing information risk. It is not a legally mandated or defined role, but is generally considered to have the following responsibilities:

- To provide board level accountability and assurance that information risks are being appropriately managed and addressed
- To ensure the maintenance of an appropriate Information Governance Framework
- To be a champion for developing a culture which values Information Governance and supports the principle of data protection by design and default
- To be an executive-level champion for the concept of information as an asset. Information is integral to the functioning of modern business and essential to delivering corporate objectives.

Plan UK Implementation

At Plan UK, our SIRO is the Chief Operating Officer and is responsible for:

- Providing Management Board and Trustee Board with a senior point of contact responsible for Information Risk
- Ensuring the data protection risk register is reviewed quarterly and risks communicated to Management Board as appropriate
- Line management of the DPO role, and ensuring the DPO's efforts are concentrated in the areas of most business value to Plan UK
- Providing challenge to Management Board, or the business, as appropriate, if it is felt that data protection compliance is not being given the importance it requires
- Providing challenge to the DPO, as appropriate, if it is felt that non-legislatively required compliance work is not proportionate to business needs
- Fostering a culture of data protection by design and default, including providing high level support to the DPO where appropriate/required
- Developing a learning culture to allow Plan UK to understand where data protection issues may arise and develop appropriate solutions to prevent problems occurring

Approved by Management Board: September 2019

APPENDIX C: Terms of Reference – Data Protection Oversight Group

Introduction

One of the key principles of the GDPR legislation is for data controllers (i.e. Plan International UK, PIUK) to be able to demonstrate their compliance. It is expected that appropriate technical and organisational measures are in place to safeguard any personal data that is processed. The ICO also expects the accountability methods and measures to be reviewed at appropriate intervals, with suitable senior management oversight.

Purpose

The purpose of the Data Protection Oversight Group is to:

- Maintain compliance with the overall framework of data protection legislative measures, for example (but not limited to) GDPR, The Data Protection Act 2018, PECR
- Oversee the organisation's data protection responsibilities in key business areas to ensure compliance, and ownership of the resulting levels of risk, including maintaining a data protection risk register
- Ensure an effective data protection compliance framework is in place and maintained and to own the organisational approach to data protection compliance including all policies and procedures within this framework
- Review work carried out or planned by the Data Group, and any issues/actions arising
- Review summary information about Data Protection breaches, Subject Access Requests, and Data Protection Impact Assessments (DPIAs) and provide input, challenge and decision making where required
- Review annual summary report to Management Board and Trustee Board, as well as more frequent reporting, as required

The Data Protection Oversight Group will review these terms of reference annually, with any proposed changes to be approved by Management Board.

Membership

- Chief Executive (Chair)
- Head of Corporate Governance (HOCG)
- Senior Information Risk Officer (SIRO, also Chief Operating Officer)
- Data Protection Officer (DPO, also Head of IT)
- Other staff members to attend as requested by the Chair

Meetings

The Data Protection Oversight Group meets quarterly for 2 hours. The HOCG (or otherwise as appointed by the Chair) organises the meetings and takes and circulates minutes and actions from each meeting. The minutes record decisions made, items formally noted and action to be taken. Additional discussions/decisions may take place by email as required.

A draft agenda will be produced two weeks before the meeting by the HOCG and circulated to all members, with a final agenda and papers sent one week before each meeting, so that all papers can be read ahead of the meeting.

Approved by Management Board: September 2019

APPENDIX D: Terms of Reference – Data Group

Introduction

One of the key principles of the GDPR legislation is for data controllers (i.e. Plan International UK, PIUK) to be able to demonstrate their compliance. It is expected that appropriate technical and organisational measures are put in place to safeguard any personal data that is processed, with suitable involvement of applicable staff.

Purpose

The purpose of the Data Group is to:

- Consider and agree the appropriate prioritisation of ongoing compliance work, e.g. updating the Register of Processing Activities (ROPA) and selection of Vulnerability Assessment initiatives
- To determine whether there are any areas where PIUK's processing of data might be improved, or Data Protection Impact Assessments may be required, supporting the Information Asset Owners (all Heads of Unit) to ensure that that their units are compliant with data legislation
- Disseminate information and learning from the Data Group meetings back to the teams within the organisation with a view to building and improving an organisational culture of data protection awareness
- Advise and support the Data Protection Officer (DPO) and Data Protection Oversight Group on data compliance issues, providing specialist knowledge, and feeding into the Data Protection risk register

The Data Group will review these terms of reference annually, with any proposed changes to be approved by the Data Protection Oversight Group, and notified to Management Board.

Membership

In line with its purpose above, the Data Group is made up of senior staff from all directorates. If staff are unable to attend, they should send an appropriate deputy in their place. Attendees must be able to communicate information to and from their directorate with respect to all Data Group matters.

- Data Protection Officer (DPO, also Head of IT) (Chair)
- Head of Individual Giving
- Head of Major Partnerships
- Head of Girls' Rights and Youth Team
- Digital Strategy & Development Manager
- Evidence, Learning and Impact Manager
- Head of Corporate Governance
- Head of HR
- Head of Finance
- Property & Facilities Manager
- IT Development Manager
- Other staff members to attend as requested by the Chair

Meetings

The Data Group meets quarterly for 2 hours. The DPO (or otherwise as appointed by the DPO, as Chair) organises the meetings and takes and circulates minutes and actions from each meeting. The minutes record decisions made, items formally noted and action to be taken. Additional discussions/decisions may take place by email as required.

A draft agenda will be produced two weeks before the meeting by the DPO and circulated to all members, with a final agenda and papers sent one at least two working days before each meeting, so that all papers can be read ahead of the meeting. Attendees are expected to bring their own hard copies of papers.

Approved by Management Board: September 2019