Data Protection Accountability Statement

Title	Data Protection Accountability Statement
Author	Peter Roberts – SIRO; ISM
Owner	Peter Roberts – SIRO; ISM
Version	1.0
Status	Approved
Approved by management board on	16th February 2022
Circulation	All staff, all stakeholders (on website)

Data Protection Accountability at Health Diagnostics Ltd.

As part of our compliance with the Data Protection Act 2018, and the UK General Data Protection Regulation [UK GDPR], Health Diagnostics has reviewed how we demonstrate accountability for our data processing activities.

Health Diagnostics is not a public authority and does not carry out large scale processing of data or data relating to criminal convictions and offences. However, our core activities do involve large regular processing of personal data and sensitive personal information, so we have 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.

Health Diagnostics has an Information Security Management System [ISMS], 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 as per the ISO 27001:2013, the international information security standard to which we are accredited. This includes specific roles such as the DPO and SIRO.

Key roles:

Senior Information Risk Owner – Peter Roberts, Head of Technical Operations
Data Protection Officers – Ametros Group Ltd
Information Asset Owners – all heads of departments are responsible for ensuring that their department 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 Health Diagnostics, 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.

IAO's are responsible for making sure that the business processes and decision making in their departments are in line with UK 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 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 for 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://healthdiagnostics.co.uk/security-privacy-privacy-policy/

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 Information Security Group (ISG) meetings with our director level representatives to ensure an effective data protection compliance framework is in place to ensure data protection risks and issues are dealt with at an appropriately senior level within Health Diagnostics.

Our compliance with ISO 27001:2013 was most recently audited in 2021 by an external organisation. We maintain related externally verified annual compliance measures such as Cyber Essentials compliance and carry out penetration testing at least annually.

Our Data Protection Officer

We use the Data protection Officer service provided by Ametros Group Ltd. The service is provided by a multi-discipline team of data protection experts that form a core DPO support team, including EU certified GDPR practitioners, lead ISO auditors, cyber security and business process management consultants

Independence

The DPO can raise issues in the way and in the manner they see fit. Our DPO is not penalised for performing their tasks or challenging the business.

Reporting to the highest level of management.

The DPO provides an annual summary report to the Management Board as well as reporting more frequently, including immediately, should the need arise (e.g. In the case off 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 Health Diagnostics' processing of personal information. Our DPO has regular contact with all members of our senior management team. Our DPO can have 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 the management board.

The DPO works closely with the SIRO who is also the head of technical operations at Health Diagnostics Ltd. As SIRO and head of technical, the tasks and focus of each role are complementary – and sitting in technical provides additional intelligence in terms of knowing about new systems or processes in development. The DPO and SIRO are encouraged to raise any conflict-of-interest concerns with the management board.

Visibility

Our DPO's contact details are included with 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.