



Data Protection & GDPR Health Check

Service Overview

Ensuring Your Data Supports Your Business

You must make the best use of today's digital information to deliver the optimal level of service and support to your customers. In a climate where all forms of data are becoming more and more valuable for clients, customers and malicious Third Parties, measures must be taken to ensure effective privacy and protection of this data whilst allowing you to use it for greatest commercial impact.

Furthermore, data protection laws and ever increasing regulatory and commercial pressure on the use of information are vital issues that impact on every organisation. The EU General Data Protection Regulation (GDPR) represents possibly the biggest change to data protection law and affects every organisation that controls or processes Personally Identifiable Information (PII) of EU customers and/or employees.

DVV Solutions understands that in order to ensure the ongoing services you offer are delivered in line with GDPR and other regulations, your organisation must first gain an understanding of the privacy risk areas you face and what exposure these risks leave you with. Not until those risks are identified and understood will you be able to mitigate those risks accordingly.

DVV Solutions are able to assist you with this burden through a comprehensive **Data Protection and GDPR Health Check** providing an independent objective assessment of your organisation's current data protection and compliance posture.

Your Data Protection & GDPR Health Check

Your Data Protection and GDPR Health Check is a business critical tool that is designed to identify how the organisation stands in relation to data protection legislation whilst also assessing the organisation's data protection posture.

- ✓ **Assessment of data processing in relation to the 6 Principles of GDPR**
- ✓ **Assessment of privacy notices and DSAR processes**
- ✓ **Assessment of your applicable GDPR policies and documentation**
- ✓ **Assessment of your processes in relation to the 8 'rights' of data subjects**
- ✓ **Assessment of technical data security capabilities**
- ✓ **Assessment of relationships with data processors**
- ✓ **Assessment of Staff training and awareness**
- ✓ **Assessment of Incident Response & Breach reporting**



The Health Check Process

DVV Solutions will undertake a comprehensive program of work in order to fully evaluate your current data protection and privacy posture and the risks to your data.

Engaging our services allows your organisation to appoint dedicated industry professionals who have the knowledge and expertise of data protection law and practices to ensure and demonstrate compliance with regulations including the Data Protection Act, 1998 (DPA) and GDPR.

Your Data Protection and GDPR Health Check will be built upon our 3 step process:

Current State Review

Evaluation of current documented policies and procedures.

Builds understanding of current state and structures in order to successfully execute a thorough assessment.

Consultation & Assessment

Face to face evidencing of current state with key stakeholders and function owners.

Develops an understanding of operational environment and practical implications of data privacy and management within the organisation.

Analysis & Reporting

Evaluates the impact and effectiveness of the data management, security and risk controls in place.

Reports on current gaps and key data risks.

Provides detailed recommendations for improvements to data management, regulatory compliance and security posture.

Performing the Health Check



A schedule of meetings and assessment activities will be agreed with the nominated single point of contact and the identified business areas. This will be reviewed in a meeting or call in advance to ensure that the interviews are with an appropriate mix of managerial and operational staff and cover all of the control areas necessary to establish an assurance rating. A draft schedule and list of the controls to be covered will be provided in advance.

While on site the assessment team will meet with staff to establish if controls are in place to ensure the organisation complies with its data protection responsibilities. This will include interviews with staff, reviewing relevant records and, if necessary, observing procedures being implemented in practice. DVV Solutions may require access to relevant staff 'desk side' where possible to understand how staff process personal data (limited to the scope provided).

Space will be usually be allocated in the schedule of interviews for testing and evidence gathering. DVV Solutions will consider the extent to which any Internal Audit department includes data protection audits in their programs of audit or compliance work to avoid duplication of work.

A nominated single point of contact will be required to be available throughout the process to provide support and exchange feedback on progress. DVV Solutions believes that regular feedback should assist both the assessor and the organisation to quickly understand and address emerging issues and concerns and help to avoid any misunderstanding.

Pre-Health Check Requirements

The following documents, if available, should be sent to the assessors prior to the fieldwork commencing.

- > Organisation Chart including Roles and Responsibilities
- > Data Protection Policy
- > Processor / Employee Confidentiality Agreement
- > Records Retention Policy
- > Subject Access Request Procedure
- > Personal Data Breach Policy and Procedure
- > Data Impact Assessment Process
- > Data Sharing Policy and Data Sharing/Processing Contract example
- > Procedure for International Transfers of Personal Data
- > Data Collection Forms
- > Fair Processing Notices
- > Any other policy you feel may be relevant to Data Protection & Privacy

Business Familiarisation & Documentation Assessment



A comprehensive assessment of the organisation's documentation in relation to data protection practices will be carried out. This will be done in order to understand operational aspects of the organisation and how they interlink with data protection practices.

Any gaps or conflicting policies will be highlighted as part of this assessment. This stage allows the assessors to familiarise themselves with business processes.

Onsite Fieldwork

At the start of the visit, we will arrange for an opening meeting with appropriate members of your senior management to explain the process to them. This provides an opportunity to discuss any issues and agree the data gathering process.

The methodology used by the assessment team during the on-site visit is primarily a written response and interview based approach. Prior to onsite fieldwork the assessment team will distribute a series of questionnaires to the single point of contact, for completion by the appropriate stakeholders/process owners for subsequent verification during the interview phase.

During the visit all assessors will make notes from interviews, observations and testing. This may be supplemented by visual inspections and examinations of selected uses of personal data within the organisation.

It is of paramount importance that questions posed by the assessment team be answered comprehensively and accurately. The questions asked, and evidence gathered, would depend on the scope areas agreed in the letter of engagement. However, there are some generic areas that are normally covered within each scope area.

Upon completion of the assessment visit, the assessment team will hold a meeting with the organisation's management. If any major concerns have been identified by the assessment team they will be highlighted at this point. As far as possible, a general overview of progress will also be given.

Administration of Engagement

Individual site arrangements for access and assessing will be channeled through a nominated contact in your organisation.



Where possible interviews will be carried out on the client's premises. With the exception of assessments and interviews undertaken at specialist technical sites that may be conducted at a pre agreed location.

A room will be made available, where possible, to DVV Solutions assessors at sites identified in the schedule to carry out interviews, when it is not appropriate to work 'desk side', or while they are not conducting interviews.

Schedule of Key Events

In order to provide you with an expectation of the overall level of effort required and target timescales to execute the program of works we provide the following outline schedule of key events and milestones in undertaking the Health Check:

- > Acceptance of proposal by client
- > Engagement letter sent to client
- > Signed engagement letter received
- > Organisation's documentation received
- > Business Familiarisation & Documentation Assessment commences
- > Scoping meeting with nominated point of contact to confirm process and schedule
- > Date of on-site visit(s) and schedule of interviews/work confirmed
- > Distribution and completion of GDPR questionnaires
- > Assessor attendance on site – fieldwork carried out
- > Health Check Report issued within 14 days of fieldwork being completed
- > Completion meeting / conference call where report is presented

Note: Schedule and timelines may be subject to final agreement and the availability of relevant parties and documentation.

Data Protection and GDPR Health Check

Scope of Work

The scope of the Data Protection and GDPR Health Check and assessment activities will assess the risk of non-compliance with appropriate data protection principles, the utilisation of Information Commissioner's Office (ICO) guidance and good practice notes and the effectiveness of data protection activities with specific reference to:

- > **Data protection governance** - The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.
- > **Training and awareness** - The adequacy of current provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.
- > **Records management** - The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of PII data records.
- > **Security of personal data** - The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.
- > **Subject access requests** - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.
- > **Data sharing** - The design and operation of controls to ensure the sharing of personal data complies with the principles of the DPA and GDPR and the good practice recommendations set out in the ICO Data Sharing Code of Practice.

Out of Scope

DVV Solutions will restrict its assessment activity to the departments and locations detailed and agreed within the scope. The Data Protection and GDPR Health Check will not review and provide a commentary on individual cases, other than to the extent that such work may demonstrate the extent to which your organisation is fulfilling its obligations and demonstrating good practice.

DVV Solutions, however, retains the right to comment on any other weaknesses observed in the course of the assessment process that could compromise good data protection practice.

Expected Added Value



Your Data Protection and GDPR Health Check is intended to address the areas of greatest risk and impact, and give you detailed guidance. As a result it can provide the following commercial benefits to your organisation:

- ✓ **Minimised Risks** – in-depth gap analysis of your existing processes will help to identify any potential risks or breaches ensuring processes are more aligned with the regulation.
- ✓ **Improved Staff Awareness** - staff and senior management will learn from each other about real life data protection issues and be enabled to develop better, standardised policies and processes. Understanding what regulations mean to their roles and the organisation will also develop greater commitment to achieving compliance.
- ✓ **Improved Management and Security of Data Processing** – data mapping exercises will give you and your team greater awareness of, and control over, the data you hold, who it is shared with, and what you need to do to protect it.
- ✓ **Greater Ability to Manage Risks** – we will help you understand how to complete a Data Protection Impact Assessment (DPIA), an important tool in helping you to identify and mitigate data risks when reviewing existing or new projects and suppliers.
- ✓ **Auditable Document Trail** – we can provide you with the necessary templates to create a document trail in place to demonstrate evidence of your efforts to achieve and maintain GDPR compliant processes and practices.
- ✓ **Improved Reputation** – by ensuring you only process data where you have the right to do so and improving the way you manage data, you will increase confidence in your brand and reduce the risk of fines and subsequent reputational damage.
- ✓ **Streamlined and Simplified Route to GDPR Compliance** – our expert team are able to navigate you through complex and time-intensive compliance processes and documentation to ensure you get the most effective and cost-efficient outcomes.

About DVV Solutions

As specialists in Data Protection, Privacy and Governance we provide our clients with a service of the highest quality in a professional, commercial and responsive manner. We aim to assist you in enabling your organisation to reach its maximum potential in line with data protection and privacy regulations.

Since 2014, we have been audited and are accredited to ISO14001 standards and in 2016 were also certified to the UK Government's Cyber Essentials Scheme.

Our ethos is to provide you the best value for money by offering the highest quality of service within a clear and consistent cost model. We do this by leveraging our extensive experience in the IT services sector and our best-of-breed technology and service partners.

Start Your Health Check Today

Let DVV solutions help you in ensuring the PII data of your Customers and Employees is secure, protected and managed within GDPR's strict regulations with a Data Protection & GDPR Health Check.

We'll deliver a cost-effective program of work that helps you to achieve the level of data protection, privacy and GDPR compliance that your business requires.

Contact us to start building your Data Protection & GDPR Health Check today.

Call Us on +44 (0) 161 476 8700