# BSI Digital Trust - Data Privacy (DP) Service

## G-Cloud 14 Service Description

Supplementary information document

Expiration of Commercial Offer

This proposal and pricing expire in 20 days from receipt.

Statement of Confidentiality

This proposal, associated quotation pricing, and functionality description in whole and in part is considered confidential information

By Royal Charter

06 May 2024

| Version | Description | Author | Date |
|---|---|---|---|
| 1.0 | Final Version | Joe Halberda | 06/05/2024 |
| | | | |
| | | | |
| | | | |
| | | | |

# Contents

# Service Overview

## Service summary

BSI Digital trust's Data Governance (DG) practice will help you navigate and solve complex data challenges around privacy, data management, data governance or eDiscovery and forensics. Our expanding global expertise provides services to meet your business' needs and enable you to build and sustain trust. That starts with your data.

## Key features

Key features of BSI Digital trust's Data Governance practice include:

- Data Protection Officer Services - nominated and virtual offerings
- Global Privacy Programme – scoping, designing & implementing scalable privacy programme
- Article 27 EU Representative - EU compliance for UK companies
- ISO/IEC 27701:2019 privacy information management system (PIMS) – implementation & audit
- Privacy by Design – guidance & expertise in privacy enhancing measures
- Privacy maturity assessments, compliance reviews and audits
- Data Subject Access Requests – scoping, finding, producing and end-to-end management
- Training – industry bespoke courses in privacy, data management and security

## Key benefits

Key benefits of the BSI Digital trust's Data Governance practice include:

- Minimizing compliance, operational and strategic risks
- Having confidence in the quality and accuracy of your data
- Meeting increasing regulatory obligations for data localization, transfers and uses
- Knowing where data is located, or with whom it is shared and why
- Enabling certainty over why data is processed
- Assuring the retrieval and production of data for regulatory deadlines
- Destroying data when it is no longer needed
- Protecting data and keeping it safe and secure
- Reacting decisively and confidently when something goes wrong with data
- High quality, independent and impartial advice from experienced, expert professionals

# Service Description

## Data Protection Officer Services

The Data Protection Officer (DPO) is an important leadership role within an organization's governance structures and is a key stakeholder in the data protection accountability framework defined by the UK General Data Protection Regulation (GDPR). The DPO oversees and monitors data protection compliance and reports independently to the senior management level of the organization. They also act as the primary point of contact for data subjects, customers, suppliers, and employees who have data protection related queries or concerns. The DPO also cooperates with the Information Commissioner's Office (ICO).

Article 37 of the GDPR specifies that the appointment of a DPO is required where an organization meets any of the following criteria:

- A public authority or body processing and controlling personal data
- Core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- Core activities consist of processing on a large scale of special categories of data

However, even if your organization is not obligated to do so, appointing a DPO or a Privacy Officer is a prudent action that helps demonstrate data protection and privacy are core strategic elements for your organization.

Appointing an in-house, independent DPO may not be feasible for many organizations as ensuring the independence requirements and finding an individual with the necessary skill set is often too difficult. A DPO must be competent in risk management, compliance, audit, information security, data protection law, data protection practices, privacy engineering, and emerging fields such as artificial intelligence, data governance and machine learning.

The tasks of the DPO, as specified in the GDPR are:

- Informing and advising management and employees of their obligations under the GDPR
- Monitoring compliance with the GDPR
- Advising, where requested, with regards to data protection impact assessments, and monitoring their performance
- Cooperating with the ICO
- Acting as the contact point for the ICO on issues relating to data protection and the processing of personal data

As part of our privacy and data protection service portfolio, our team of experienced consultants can support you in all aspects of your organization's requirements of a DPO or Privacy Officer.

BSI provides tailored Data Protection Officer advisory services supporting organizations to meet their operational data protection compliance obligations. BSI's DPO services support the implementation of frameworks, policies, objectives, solutions and plans to improve the maturity of data protection. BSI uses a risk-based approach to compliance that is data subject-focused, operational, and pragmatic.

**Features**

- Nominated DPO service – including registration of BSI with ICO as your named Data Protection Officer
- Virtual DPO service – in support of your in-house DPO or privacy compliance function
- Scalable support tailored to your organization's data protection maturity and risk appetite
- Independent advice that that is based on a cross-functional team of consultants and up-to-date monitoring of emerging practices, legislation, and regulatory developments
- Phased approach including a dedicated mobilization period adopting on a risk-based approach to identify gaps in compliance and build a remediation and compliance monitoring plan
- Dedicated access to the DPO team
- Escalation and out-of-hours support options for regulatory, breach or other urgent matters

**Benefits**

- Meet the independence requirements for the DPO role without compromising existing internal duties or roles
- Reduce the overhead costs associated with employing an internal DPO
- Eliminate the key person dependency risks associated with an internal DPO
- Quickly access specialized, skilled, and experienced privacy, data management, forensics, and security consultants in the event of a personal data breach, supervisory authority investigation or other impact event
- Reduce the risks of non-compliance, breach, regulatory censure, and financial loss

## Global Privacy Programme

Global data protection and privacy legislation is evolving at a pace never seen before. Organizations face a landscape that frequently shifts based on international political agreements, national legislative changes and regulatory decisions and interpretations. Privacy compliance is no longer an afterthought, or a checkbox exercise that organizations can address once and move on. It is a continuous iterative compliance challenge that must be embedded into the DNA of organizations from top to bottom. This mandates a programmatic approach to addressing privacy and focusing on embracing privacy and data protection as enablers of trust.

BSI can support your organization design, develop, implement, operate and mature a global privacy programme tailored to your geographic footprint. Our experienced data protection experts support organizations all across the UK and around the world to meet their operational data protection compliance obligations within the context of global data transfers, emerging legislation, evolving regulatory decisions and implications.

Establishing a global privacy programme is a strategic decision that enablers the achievement of practical outcomes including creating competitive advantages, improving and maintain customer trust, increasing compliance, increasing resilience to legislative and regulatory changes and enabling scalable management of regional or global growth.

The key focus of BSI's global privacy programme services is to create a baseline standard for privacy within your organization from which you can flex to meet regional or national variations. Adopting this approach

means you can focus on your business whilst BSI manages a scalable privacy program to support your core activities, not hinder them.

BSI's global privacy programme services are grounded in the reality of your organization's risk appetite, is baselined on the legal compliance requirements, international frameworks, and privacy-by-design approach to embed privacy at the core of your operations and improve the maturity of data protection.

BSI uses a risk-based approach to compliance that is data subject-focused, operational, and pragmatic.

Our team monitors the evolving data protection and privacy landscape to ensure our team can provide swift, pragmatic and effective advice that is tailored to your organization's technology, cultural, industry and privacy-maturity environments.

Key compliance focus areas include:

- Design, implementation and monitoring of required technical and organizational measures
- Restrictions on international data transfers
- Transfer impact assessments
- Data localization and data sovereignty
- Privacy and data protection by design & default
- Enhanced and evolving rights for data subjects
- Increased territorial scope of new and updated legislation
- Strict requirements for data breach notifications
- Special categories of personal data
- Surveillance and profiling of data subjects
- Demonstrating compliance to regulators and customers

**Features**

- Tailored to your organization's legislative and compliance footprint
- Programme objectives, timelines and workstreams customized to your business strategy and data processing activities
- Adopting a risk-based approach to privacy compliance
- Continuous monitoring of evolving privacy and data protection compliance landscape
- Programme governance, reporting and progress monitoring

**Benefits**

- Uplift privacy as a strategic focus and imperative for your business success
- View privacy as an enabler for competitive advantage
- Build and sustain customer trust in your brand, your products/services and your approach to doing business
- Implement a scalable for flexible approach to privacy that can adapt to the evolving nature of privacy legislation and regulation
- Create a culture of privacy, that builds privacy and data protection by design into the essence of your operations

## Article 27 EU Representative Services

One curious aspect of the EU GDPR is that it applies outside the EU's border under certain circumstances including for certain UK based organizations. Article 27 of the EU GDPR mandates that a UK company must have an EU-based Representative when it does not have an establishment in the EU and either targets its goods or services into the EU, or monitors EU-based data subjects.

The Representative has several following important regulatory responsibilities including acting as the contact point for data subjects and the supervisory authorities in the EU; providing any information the EU Supervisory Authorities require for the performance of their tasks; and maintains a copy of the Article 30 Record of Processing Activities (RoPA) of the non-EU organization.

BSI's global data protection and privacy consultants can help your organization meet the EU GDPR Article 27 obligations in an efficient and cost-effective way, allowing you to focus on your business.

**Features**

- EU-based consultants that can provide Article 27 Representative services to UK-based companies
- Register BSI's EU address as your EU Representative address
- Name BSI in your privacy policy as your point of contact in the EU
- Regular touch points to ensure the RoPA is maintained up to date in line with Article 30, EU GDPR
- BSI can undertake mandated additional tasks, if required and agreed

**Benefits**

- Reduce the risks of non-compliance with EU GDPR
- Facilitation of communication between EU-based data subjects and your organization, to make the exercise of data subjects' rights effective
- Cooperation EU-based supervisory authority(s) regarding any action taken to ensure compliance with the EU GDPR
- Facilitation of any informational or procedural exchange between a supervisory authority(s) and your organization
- Access specialized, skilled, and experienced data protection consultants
- Ensure your EU-based compliance obligations are met in a cost effective and efficient way

## ISO/IEC 27701:2019 Privacy Information Management System (PIMS)

BSI offers support for the implementation of ISO/IEC27701 and a range of HMG Accreditation approaches for cloud services and service compositions including cloud services in support of transition and ongoing operation. The service is flexible and can range from strategic advice, through to the implementation of policies and procedures. ISO/IEC 27701 helps businesses put the protection of personal data at the core of their operations as an extension to an Information Security Management System (ISMS).

Today, in this highly interconnected world, it is important for organizations to ensure that personal data is managed in line with the evolving compliance landscape. The Government sector process large volumes of personal and other sensitive data, and relies on the confidentiality, integrity, and availability of its systems to support the delivery of core business functions. Increasingly, it is leveraging the benefits of using Cloud computing, with services being commoditised and scalable, but this also brings new privacy challenges.

BSI offers a full range of NCSC Certified Cyber Professional (CCP) roles to assure cloud services through ISO 27701 certification and public sector accreditation schemes.

BSI is experienced in conducting Information Assurance (IA) audits as well as reviewing privacy and security policy documentation. We have a large team of experienced data protection and privacy consultants, with industry leading CIPP/E, CIPM, CIPT, FIP, PECB and ISACA qualifications, ISO/IEC 27001 Lead Auditors, as well as CCP IA Auditors and PCI DSS QSAs.

We frequently undertake process audits and policy reviews of key policies and procedures, with a view to identifying any missing policies or any requiring updates, according to the client's personal data and privacy compliance requirements.

BSI offers consultancy for implementing the ISO/IEC 27701 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management, as required for certification. The approach typically involves:

- Defining scope of the PIMS
- Gap Analysis to identify required improvements
- Developing a Risk Management framework
- Policy, Standards and Guideline creation
- Advice on appropriate controls
- Audits, either pre-certification or within an ongoing ISO 27001 programme.
- Training and Awareness
- Privacy Incident Management and Response

**Features**

- Privacy Information Management System (PIMS) strategy, development, and implementation
- Produce and agree PIMS Scope and Policies
- Risk assessments methods supported include IS1, IRAM, IRAR and CRAMM
- Carry out Risk Assessment and produce Risk Assessment Report
- Conduct initial Gap Analysis and produce the Statement of Applicability (SoA)
- Establish and operate Governance Forums including Terms of Reference (ToR)
- Produce risk acceptance and risk treatment plan and PIMS / ISMS procedures
- Conduct internal compliance assessments and audits
- Provide operational privacy and security management, including incident and protective monitoring management
- Review operational privacy reports and attend security / privacy forums and management reviews
- Privacy incident management and investigation

**Benefits**

- Service suitable for public, private, community and composed cloud solutions
- Experience with assurance approaches including MoJ, Multiple Police Services, DfES and PSN
- Experience with solutions including Skyscape, AWS, Azure, and Office 365

- Service resources have worked with multiple UK public sector clients
- Consultants qualified as ISO27701 Lead Auditors/Implementers and CCP IA Auditors
- Carried out by qualified consultants
- ISO 27701 Lead Auditors / Implementers
- CCP Security and Information Risk Advisor (SIRA)

## Privacy / Data Protection by Design and Default

Increasingly, modern privacy and data protection laws mandates that organizations embed data protection and privacy by design and default into their products, services and operations. Whilst much focus is placed on undertaking proactive data protection impact assessments (DPIAs) or Privacy Impact Assessments (PIAs), a true "by-design" approach requires significantly more than documented assessments against regulatory compliance.

Shifting mindsets from compliance to a "by design" approach requires a radical change in processes. Moreso, however it also needs a significant change in culture and commitment from senior management all the way through to designers, product engineers, system developers, programme and project managers.

Adopting a by-design approach to privacy involves putting the right to privacy at the forefront of your organization's considerations when designing, developing or implementing new systems, solutions, services or products.

BSI can assist your team to create a methodical and systematic manner to introduce complementary processes into existing change processes that assist in the early identification of possible potential and actual privacy violations; assess alternative approaches to achieve similar or better outcomes and realize both privacy protections and commercial objectives.

BSI has significant experience in helping organizations make that step-change, adapt existing methodologies and approaches to project management, change management or business development, and embed privacy-by-design across the engines of change.

Our operational privacy consultants have significant experience in privacy engineering, supporting product operations, privacy specialists, in-house DPOs and privacy functions strengthen and embed a by-design and default methodology that enables and sustains trust.

**Features**

- Access a team of privacy consultants with pragmatic and real-world experience in privacy enhancing technologies and privacy enhancing measures
- Agile approach to privacy engineering and privacy/data protection by design and default
- Proactive and reactive mechanisms to identify privacy threats and violations
- Experience in securing senior management buy-in and support for strategic changes to change and development processes
- System, platform and technology agnostic

**Benefits**

- Embed a culture of privacy and data protection by design and default
- Leverage privacy as a competitive advantage

- Embed scalable assessment, engineering and privacy protecting methodologies
- Create, sustain and grow customer and public trust
- Enable compliance by design and default
- Prioritize data subject rights

## Privacy Maturity Assessments, Compliance Reviews and Audits

Data protection and privacy compliance is not a one-time occurrence, it requires ongoing check points, and validation to ensure that risks are managed, and compliance is maintained. Providing senior management with visibility of the overall and trending compliance levels is a tried and tested method of improving maturity and reducing risk.

BSI's team of data protection and privacy consultants have considerable experience in leveraging the "Three Lines of Defence" (3LOD) model approach to provide first-, second-, and third-line assurance to organizations over their operational data protection and privacy compliance capabilities.

BSI's approach is collaborative and tailored to our customers specific compliance needs and risk-appetite. Adopting both jurisdiction-specific legislation and establishing and emerging international standards to form the baseline for our independent assessments, we can assist you in identifying current compliance gaps for remediation using a prioritized and risk-based approach.

BSI can provide tailored audit and assessment services that align with your assurance requirements including, for example:

- NIST Privacy Framework v1.0 Maturity Assessment
- AICPA/CICA Privacy Maturity Model
- ISO/IEC 27701 Privacy Information Management System
- Fair Information Privacy Principles (FIPPs)
- Legislative compliance including, but not limited to:
    - UK GDPR, PECR
    - EU GDPR, ePrivacy
    - US legislation (e.g. CA CCPA, CA CPRA, HIPAA, COPPA,
    - Australia's Privacy Act
    - New Zealand's Privacy Act
    - Brazil's LGPD
    - South Korea's PIPA
    - China's PIPL
    - Singapore's PDPA
    - Japan's APPI

BSI's operational experience of adopting either first line, second line or third line of defence approaches means we can expertly report using your desired report and assessment templates or leverage BSI's own report templates to ensure the intended outcomes are maximised and the desired audience receives the information as effectively as possible. We have significant experience as outsourced internal auditors,

providing independent reviews, and supporting due diligence assessments as part of merger and acquisitions

BSI can provide a tailored compliance assessment for any situation, for example:

- Internal audit committees
- Senior management
- Merger and acquisitions
- Compliance monitoring
- Independent compliance reviews
- Legislation and regulatory changes
- Maturity improvement plans

**Features**

- Tailored assessment and reporting approaches based on your organization's needs
- Assess compliance against international standards, global legislative requirements or international good practice in privacy
- Secure fact and evidence-based findings to prepare improvement roadmaps, maturity improvement plans or audit remediations
- Provide assurance to senior management, audit committees, customers, or in merger and acquisitions (M&A)

**Benefits**

- Secure customized audit, compliance or assessment services
- International operational experts with framework and standards implementation and operationalization experience
- Leverage a truly independent perspective on your compliance or audit need
- Secure comprehensive assurance for your audience, whether internal, external or as part of due diligence compliance assessments

## Data Subject Access Requests (DSARs)

BSI can provide advice and assistance on all stages of a Data Subject Access Request, from assisting with locating potentially relevant data and selecting the most appropriate keywords to identify documents that require review, through ensuring that the document review is fast and efficient to providing searchable redacted PDF output for the relevant documents to be handed over to the subject.

- **Scoping support** – where could company staff have stored documents relevant to the request and what keywords are appropriate to use to identify documents for review
- **Review support** – potentially relevant documents will be deduplicated and uploaded to a hosted review platform purpose-built to speed up the review process. AI and keywords can be used to reduce the document set further
- **Redaction support** – automatic redactions are available for use when redacting specific names or phrases as well as for credit card numbers, phone numbers and other text strings of a set format.

Additionally, manual redactions are quick, efficient, and done in a manner that prevents accidental disclosure of redacted text

- **Production** – can be set to native files, redacted searchable PDFs or a mixture of the two to give the subject the most usable data set possible

## Training

We provide a range of accredited training courses that can help you get the knowledge and skills you need to build resilience around your information security and data management. From beginner to advanced courses, we have got you covered. Depending on your requirements, we can deliver training in several ways with BSI approved training that can:

- create a competitive advantage
- improve critical knowledge across the organization
- maintain credibility within your industry

Courses that can be accessed include the following:

**Incident Response & Digital Forensics**

- Certified Incident Handler V2 (ECIH)
- Computer Hacking Forensic Investigator (CHFI)
- ICS Security Incident Response Fundamentals
- Incident Response for Managers and DPOs
- ISO 27035 Lead Incident Manager

**Information Security Management**

- Certified Chief Information Security Officer (CCISO)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- NIS Directive Fundamentals

**Privacy & Data Protection**

- Certified Data Protection Officer (CDPO)
- Certified Information Privacy Manager (CIPM)
- Certified Information Privacy Professional Europe (CIPP/e)
- Certified Information Privacy Professional / US (CIPP/US)
- Certified Information Privacy Technologist (CIPT)
- GDPR Foundations
- GDPR Implementor / Self Assessor
- PrivSec Champion Foundations