



THE GDPR READINESS ASSESSMENT

KEY BENEFITS & DELIVERABLES

- **Draft report:** A draft report will be submitted within 21 days of the site visit which will be discussed with the organisation's representative to make corrections and/or challenge any assumptions and opinions.
- **Final RAG report:** Which will contain an assessment of information processing compliance and risk supported by objective evidence acquired through the desk research, site visit and other relevant discussions and sources. The report will contain a RAG-rated summary of compliance risks and an action plan outlining the tasks that need to be implemented to mitigate risks and/or achieve or improve compliance.

KEY SERVICE COMPONENTS

Service Commencement

An initial scoping exercise will be undertaken to determine whether the data pertains to, for example, customers, patients, tenants, staff and/or suppliers. The scoping will also consider whether the organisation is acting as a data controller or data processor, or both, either for itself or a third party. The exercise will also establish the reasons for the data's collection, for example sales or marketing, business operations or direct communication.

Service Delivery

Having determined which documentation will be required from the scoping exercise, an initial, desk-based review of any public facing strategic documentation will take place. This may include ICO Registration, privacy policies, data collection forms and methods and procedures related to information governance.

This will be followed by an on-site assessment conducted over an agreed number of days to meet with the organisation's employees and/or volunteers to review the data processing activities and practises.

Service Methodology

The aim is to find out in informal discussions what data is being processed, how it is obtained, what is done with it, who it might be shared with etc. This is done exclusively for the processing of Personal and Special categories of Personal Data as defined by the GDPR. This may include CRM records of customers, email systems, CCTV systems, staff records etc. – any data being processed that enables the person to be identified.

SERVICE DESCRIPTION

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). From 25th May 2018, affected organisations will be held accountable for a privacy-by-design approach to collecting, processing, storing and exporting EU citizen's personal details to the point of explaining to the Information Commissionaires Office (ICO) that the people, processes and technology in place were risk-assessed and appropriate.

This approach needs to consider and take into account: -

- the specific purpose for which the data is being collected
- the legal and compliance status of any entity to which data is being transferred to or accepted from
- ensuring the data is accurate and up to date
- vetting of internal staff to assure they are sufficiently responsible to process EU citizen's data
- vetting of any 3rd parties processing or storing data on behalf of the organisation
- where applicable, the appointment of appropriately skilled Data Protection Officers to the board
- to provide, on demand, the data collected, the reason the data was collected and all supporting material in both human and machine-readable formats within one month of the demand
- permanently erasing all collected data under the citizen's right to be forgotten or when the data is no longer required
- the technology, and its architecture, used to process or store the data
- having an Incident Response Plan in place should the data be compromised
- notification of a breach within 72 hours of the breach's discovery unless it can be demonstrated that the breach poses no risk to individual's data
- penalties of up to 20 Million Euros or 4% of the organisation's global turnover, whichever is the greatest

Working with our preferred partners, SecureData will perform a comprehensive review of the state of an organisation's readiness to comply with the GDPR. The review will result in a high-level action plan detailing the actions that need to be taken to ensure that appropriate measures have been taken to be compliant.



WHY SECUREDATA

Cybersecurity specialists

SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise

Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight

SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights

Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services

We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.



ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.



@SECUREDATAEUROPE



@SECURAEU

WWW.SECURAEU.COM



@SENSEPOST



@SENSEPOST

WWW.SENSEPOST.COM

