THE BUNKER
Part of the CYBERFORT group

FACTSHEET

GENERAL DATA PROTECTION REGULATION (GDPR) SERVICES

INTRODUCTION

The General Data Protection Regulation (GDPR) comes into effect on 25th May 2018 and introduces some new requirements as well as enhancing those existing in the 1995 EU Data Protection Directive and related member state legislation (e.g. the UK Data Protection Act 1998).

SIGNIFICANT CHALLENGES

DATA SECURITY

The data controller and the data processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk.

BREACH NOTIFICATION

Data controllers must notify the supervisory authority (e.g. Information Commissioner's Office (ICO)) within 72 hours of awareness of a breach. If considered high risk, individuals affected may also have to be notified, depending on the circumstances.

THIRD PARTY MANAGEMENT

Data controllers must only use data processors that provide sufficient guarantees of their abilities to implement the technical and organisational security measures necessary to meet the requirements of GDPR.

SUBJECT ACCESS REQUESTS

The data subject shall have the right to be supplied with a copy of their personal data, usually within one month of it being requested and free of charge.

DATA PORTABILITY

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

PRIVACY IMPACT ASSESSMENT

An impact assessment may be required before processing any potentially high risk data, which can identify the mitigating security controls required to reduce risk to acceptable levels.

DATA PROTECTION BY DESIGN

The principles of data protection by design and data protection by default are to be applied when developing, designing, selecting and using applications, services and products that process personal data.

RIGHT TO BE FORGOTTEN

The data subject should have the right to be forgotten where the retention of such data is not necessary.

Telephone: 01304 814800 Email: info@thebunker.net

OVERVIEW OF GDPR SERVICES

Organisations are currently in varying stages of readiness for the Regulation, ranging from not knowing how it will affect them, to being in the latter stages of a GDPRcompliance programme.

The Bunker can support organisations at every stage of the compliance journey, through assessments of current compliance readiness; gap analysis of planned or implemented controls; and a full range of GDPR focused services including Data Mapping, Incident Response, Privacy Impact Assessments, Training & Awareness, and Virtual Data Protection Officer.

The Bunker are specialist information security professionals with knowledge and experience across many industry sectors and a successful track record of delivering information security and compliance programmes to global organisations.

Read on for more information on our services.

GDPR GAP ANALYSIS

- Provides clarity to customers unsure of their current GDPR readiness or scope
- High level assessment to determine areas requiring further focus
- Completion is dependent on organisational scale and complexity, volume or types of records and a partial or full analysis
- Typically, will include an assessment of:
  - Customer's understanding of their GDPR compliance scope and impact and examination of data flow maps and diagrams
  - Data classification policy and handling process
  - Third party processors' management e.g. security assessments (pre-contract and on a regular basis), contract appraisals
  - Information security policies and procedures
  - Inventory of assets and technologies in scope
  - Locations where personal data is processed including third parties
  - Breach / incident handling
  - Risk management framework
  - Implemented security controls and processes
- Output will be a gap analysis report of existing processes and controls, and identification of additional activities

GDPR PROGRAMME REVIEW

- For customers that have instigated a GDPR programme or have begun mitigation
- Determine adequacy of existing programme and/or provide support
- Production of data flow maps showing the collection, storage, usage, sharing/transfer, archiving, and deletion of personal data
- Output will be a report of planned and implemented GDPR mitigations, prioritised roadmap of remediation activities, and identification of additional activities recommended

GDPR AUDIT

- For customers that have completed a GDPR mitigation programme or are at the later stages of it
- In-depth assessment to determine the adequacy of the GDPR programme
- Timescales dependent on scope
- Will include the same scope as the programme review but with audited evidence of implemented controls
- Output will be an audit report describing evidenced controls and The Bunker's opinion of the client's likely compliance to GDPR
- May also include identification of any additional activities recommended

TRAINING AND AWARENESS

- The Bunker can create and present awareness material on GDPR Principles, compliance requirements and potential risks
- The material and delivery can be tailored to specific audiences from board members, to general employees and third parties
- Business units (IT, finance etc.) can be targeted individually with specifically relevant training if preferred

Telephone: 01304 814800 Email: info@thebunker.net

INCIDENT MANAGEMENT PROCESS REVIEW

Early identification and evaluation of breaches is essential as well as a timely response.

This service provides the customer with the confidence that incidents are managed appropriately to enable identification and confirmation of a breach and meet the need to notify the supervisory authority within the required 72 hours specified in GDPR.

The assessment can include:

- Review of existing event logging and alert notification in place where personal information is processed
- Review of incident management policies, standards and processes (including third parties processing data on behalf of the customer)
- Create and facilitate an incident response drill, to assess—through safe execution of real-world scenarios—the adequacy of existing architectures, procedures, and training
- Areas for improvement and potential solutions identified and documented

WHY ENGAGE A BUNKER VIRTUAL DPO (VDPO)?

The Bunker can create and implement vendor assessment questionnaires and review processes for evaluating security controls of third parties that will be processing personal information on your behalf.

The assessments should be performed at initial engagement with third parties as part of contractual requirements and on a regular basis (such as annually) to ensure the continued adequacy of security controls.

The service may also include on-site auditing of vendor controls, and penetration testing and/or vulnerability assessment services if requested.

VIRTUAL DATA PROTECTION OFFICER

Many organisations have not considered the role of a Data Protection Officer (DPO) at all; or that the existing role has no gravitas; or it sits within an area of the business where it has little or no effectiveness.

WHY ENGAGE A BUNKER VIRTUAL DPO (VDPO)?

To provide a level of independence where there are no conflicts of interest

Politically neutral and not easily influenced

Provides a highly skilled and knowledgeable resource, where that skillset or knowledge is not available internally

Where creating a full-time role internally is not a viable option

WHAT CAN A VDPO DO FOR ME?

- Help you understand the impact of legislation and regulation on your organisation
- Implement the data protection framework or improve its effectiveness
- Conduct periodic assessments, including assessments of your third parties
- Drive the adoption of a proactive data protection culture, including provision of training and awareness
- Handle subject access requests and deal with data breaches
- Interface with the ICO or other supervisory authority
- Support key projects where “privacy by design” is a necessary consideration
- Support readiness for GDPR and ongoing compliance
- Conduct data breach crisis management exercises
- Review adequacy of contracts
- Monitoring and reporting of data protection activities and control effectiveness

Telephone: 01304 814800 Email: info@thebunker.net