Information Security Forum

PREPARING FOR THE GENERAL DATA PROTECTION REGULATION

IMPLEMENTATION GUIDE

The European Union's General Data Protection Regulation (the GDPR) brings data protection legislation into line with new, previously unforeseen ways in which information is used today. It applies to most organisations handling European personal data, thereby unifying data protection law for all EU member states.

The GDPR will give customers, employees and contractors (collectively referred to as data subjects) the right to demand an extract of personal data held on them by a business, request it to be passed onto a competitor, or insist it is deleted from wherever it is stored.

The way personal data is processed will be paramount. Significant fines and civil penalties, even operational intervention, await organisations that fall foul of the considerable powers vested in supervisory authorities. The need for businesses to prioritise data protection and information security has never been greater. A well-funded, well-governed, enterprise-wide GDPR compliance programme will demonstrate an organisation's commitment to data protection and security. The ISF Approach for GDPR Compliance provides a structured method and practical guidance for doing just that.

Data protection should not be seen solely as a burden. The GDPR presents organisations with an opportunity to move compliance programmes beyond risk reviews and data analysis to deliver tangible operational change and competitive advantage.

INTRODUCING THE ISF APPROACH FOR GDPR COMPLIANCE

A

The ISF Approach provides a structured method for achieving sufficient levels of compliance with the GDPR requirements. It presents good practice for guiding a GDPR compliance programme, including practical actions, supported by insightful tips from leading organisations. It is supplemented with reusable templates to accelerate demonstrative compliance.

The GDPR Implementation Guide presents the ISF Approach in two phases:

Phase A | **PREPARE** by discovering personal data, determining compliance status and defining the scope of a GDPR compliance programme.

Phase B | **IMPLEMENT** the GDPR requirements to demonstrate sufficient levels of compliance by May 2018.

B

B.1 Satisfy role requirements

B.1.1 Designate an appropriate data protection officer

B.1.2 Assign roles and train staff

B.2 Protect personal data

B.2.1 Apply data protection by design and by default

B.2.2 Apply appropriate security to data processing

B.3 Manage data protection impact assessments (DPIAs)

B.3.1 Identify when DPIAs need to be conducted

B.3.2 Conduct DPIAs on specified personal data processing

B.3.3 Determine how DPIA findings will be addressed

B.4 Demonstrate lawful processing

B.4.1 Determine legal basis for processing personal data

B.4.2 Obtain and revalidate consent of data subjects

B.4.3 Handle processing of special categories of personal data

Leading organisations are looking beyond compliance, by extending the breadth of GDPR compliance programmes to leverage additional benefits. Examples include:

- consolidating activities into broader information governance programmes
- embedding information security into the design of business applications and technical infrastructure
- improving data protection and privacy practices
- extending information security's reach within the business.

PREPARE
for GDPR compliance

A.1 Discover personal data

A.1.1 Define personal data

A.1.2 Maintain records of personal data processing

A.2 Determine compliance status

A.2.1 Conduct data discovery exercise

A.2.2 Perform GDPR requirements gap analysis

A.3 Define GDPR implementation scope

A.3.1 Identify key GDPR compliance activities

A.3.2 Create GDPR compliance plan

There are six principles relating to the processing of personal data and although these principles are not new, they provide individuals with greater rights over their personal data and assign responsibility to organisations for upholding these rights.

Article 5: Principles relating to processing of personal data

Personal data shall be:

a. processed lawfully, fairly and in a transparent manner

b. collected for specified, explicit and legitimate purposes

c. adequate, relevant and limited to what is necessary

d. accurate and, where necessary, kept up to date

e. kept in a form which permits identification of data subjects for no longer than is necessary

f. processed in a manner that ensures appropriate security of the personal data.

IMPLEMENT
a GDPR compliance programme

B.5 Uphold data subject rights

B.5.1 Resolve requests from data subjects upholding their rights

B.5.2 Demonstrate transparency of personal data processing

B.5.3 Respond to subject access requests

B.5.4 Support rectification of personal data

B.5.5 Apply restrictions on personal data processing

B.5.6 Handle objections to processing of personal data

B.5.7 Enable personal data portability

B.5.8 Erase personal data as requested by data subjects

B.5.9 Investigate objections to automated decision making

B.6 Meet data transfer requirements

B.6.1 Establish process for managing personal data transfers

B.6.2 Protect cross-border transfers of personal data

B.7 Respond to personal data breaches

B.7.1 Identify suspected data breaches

B.7.2 Investigate personal data breaches

B.7.3 Report personal data breaches to supervisory authorities and data subjects

WHERE NEXT?

The Guide is intended primarily for data protection and privacy practitioners, IT, information risk and security professionals responsible for (or supporting) a GDPR compliance programme.

Organisations should consider the ISF resources related to this Guide including ***Preparing for the General Data Protection Regulation – Digest***, ***The Standard of Good Practice for Information Security 2016*** and ***Protecting the Crown Jewels: How to secure mission-critical information assets***.

The ISF encourages collaboration on its research and tools. Members are invited to join the vibrant **Preparing for the General Data Protection Regulation** community on ***ISF Live*** to share their experience and discuss the findings and recommendations presented in this Guide.

Consultancy services from the ISF provide Members and Non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

The Guide is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members interested in purchasing the Guide should contact Steve Durbin at steve.durbin@securityforum.org.

CONTACT

For further information contact:

Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953800
steve.durbin@securityforum.org
securityforum.org

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

DISCLAIMER

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.

REFERENCE: ISF 17 06 02 | **CLASSIFICATION:** Public, no restrictions