MISSING THE LINQ

GDPR PREPARING FOR THE NEW REGULATIONS

A 12-Step Guide

ABSTRACT

With the final text of the regulations released, organisations should start planning for the changes now. This 12-step guide will help you to prepare for the European General Data Protection Regulations

MISSING THE LINQ 2017

Data Protection

TABLE OF CONTENTS

EUROPEAN GENERAL DATA PROTECTECTION REGULATION

A 12-STEP GUIDE TO PREPARE FOR THE NEW REGULATIONS

INTRODUCTION

If you're a Small to Medium sized Enterprise, and you handle personal data in some way or you use a third party to process your data then you may be interested in knowing that the EU are about to change the legislation concerning Data Protection.

The Information Commissioners Office (ICO) has recently released a 12-step plan for preparing for the European General Data Protection Regulations. This simple guide will give a basic introduction of what steps you should be taking to address your organisations data privacy risks.

Read this guide and start making preparations for the new legislation.

If you want more detailed information or help in jump starting your data protection process then go to our website www.missingthelinq.com for more information or send us an email at contact@missingthelinq.com

Or go to www.ico.org.uk for further information

STEP 1- STAFF AWARENESS

Launch a staff awareness programme

Staff must be made aware of the changing laws and the impact that a data breach may have under the new regulation.

Take the opportunity to bring them up to speed, through information sharing meetings, meet-ups also review the organisations risk register. Ensure any communications are documented and published either via email or intranet.

STEP 2 - INFORMATION AUDIT

Audit and document the information you hold

Organisations should have a clear understanding of the personal data they hold, where it came from and who it can be shared with.

An information audit is a key part of the data compliance requirements and should be performed on a regular basis not just part of this guide. It will also form part of the accountability principle, requiring organisations to show how they comply with the data protection principles.

STEP 3 - PRIVACY INFORMATION

Review and update privacy information

Organisations need to review their privacy notices and develop a strategy on how they gather and share personal data in accordance with the new regulations. This includes any disclaimers or notices on websites, as well as contracts in place with customers and third-party organisations.

The regulations also include a need to explain the legal basis for processing the data, data retention period and an individual right to complain to the monitoring body if there is a problem.

STEP 4 - INDIVIDUAL RIGHTS

Procedures should also consider an individual's rights

The new regulations cater for the individual rights to be forgotten, it therefore essential that any organisation has procedures in place to cater for an individual right to have their data deleted.

Other rights for the individual under GDPR will be;

- Subject access
- Have inaccuracies corrected
- Have information erased
- Prevent direct marketing
- Prevent automated decision-making and profiling
- Data portability

Data portability is an enhanced form of subject access and organisations must be able to respond to requests for personal data records, which will need to provided in a commonly used format.

STEP 5 - SUBJECT ACCESS REQUESTS

Update subject access request procedures

It is advised that organisations update their procedures to be able to handle data requests based on new and revised timescales, as well as be able to provide additional information as may be requested.

Organisations will NOT be able to charge for complying with a request, will have a month to comply NOT 40 days. Additional information will need to be provided to people making the requests, such as data retention periods and right to have inaccurate data corrected.

STEP 6 - LEGAL BASIS FOR PERSONAL DATA PROCESSING

Establish a legal basis for processing data

Organisations should analyse and review the reasons for processing any personal data, and document and confirm that there are solid legal grounds on which to do so.

The legal basis for processing personal data will need to be explained in the privacy notice and whenever a subject access request is processed. All of which needs to be documented to meet the accountability requirements.

If unsure organisations should take legal advice where necessary.

STEP 7 - CONSENT

Review consent mechanisms

Organisations should review and update the mechanisms on which they seek, obtain and record consent for processing personal data.

Consent has to be a positive indication of agreement to personal data being processed, it cannot be inferred from pre-ticked boxes, inactivity or silence. Consent also has to be verifiable.

STEP 8 - CHILDREN'S DATA

Update procedures for processing data about children

If as organisation you process data about children, or have data which is age related, the you should implement systems to verify individuals ages and to seek parental or guardian consent for any child data processing.

For the first time the GDPR will bring in special protection for children's data processing, in particular for commercial internet services such as social networking. In the UK children - this probably be defined as anyone under 13, will require parent or guardian's consent. Note any privacy notice must be written in language that children can understand.

STEP 9 - DATA BREACH PROCEDURES

Implement procedures for handling data breaches

The GDPR will bring in a breach notification duty across the board. Organisations should implement procedures that will enable them to

- Detect
- Respond
- Investigate

Personal data breaches according to the requirements set out in the regulation.

Assess the types of data the organisation holds and documenting which ones would fall within the notification requirement if there was a breach.

STEP 10 - DATA PROTECTION BY DESIGN

Incorporate data protection and privacy by design

Organisations need to ensure that they implement privacy by design in their processes and procedures. Any applications which are used need to have built-in security and encryption.

Privacy Impact Assessments (PIAs) procedures will need to be implemented, whilst it does not need to be carried out a PIA is required in high-risk situations, e.g. where new technology is being deployed.

STEP 11 - DATA PROTECTION OFFICER

Appoint a data protection officer

Organisations should appoint a data protection officer if they have more than 250 staff, or whose activities involve regular and systematic monitoring of data subjects on a large scale. However, for smaller organisations it would be good practise to have a nominated individual who has the role of data protection.

STEP 12 - INTERNATIONAL

Determine the data protection authority for your organisation

Organisations need to determine which data protection supervisory authority they should report to. For UK based organisations this will be the ICO, however for international organisations they will need to identify the appropriate authority in the country of preference.

In a traditional headquarters model, it easy to determine, for complex multi-site organisations where decisions about different processing activities are taken in different places it is more difficult. If unsure map out where most of the significant decisions about data processing are taken – this will determine the main establishment.

Missing the Linq
9 Farncombe Lane
Oakwood
Derby
DE21 2AY

Registered in England and Wales
No. 9832076

WEB: www.missingthelinq.com EMAIL: contact@missingthelinq.com