GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) was introduced in May 2018 to replace the UK Data Protection Act 1998. The aim of the GDPR is to strengthen the rights of individuals and transform the way personal data is collected, shared and used globally. So regardless of whether you are a Data Controller or a Data Processor you will have increased responsibilities under the new regulation.

HERE IS A REMINDER OF THE KEY CHANGES

BREACH REPORTING

Mandatory breach reporting forms part of the new regulation. Data Controllers and Data Processors are required to report breaches to the ICO, and in some cases the Data Subject, within 72 hours of becoming aware of it.

BREACHES MUST BE REPORTED WITHIN

72 HOURS

PENALTIES FOR BREACHES

The consequences of a breach have increased in severity with fines of up to £17m or 4% of global turnover.

£17m

OR 4% OF GLOBAL TURNOVER

NEW RIGHTS FOR INDIVIDUALS

DATA SUBJECTS RIGHTS

The Data Subject has increased rights over the use of their personal data with the introduction of the Right to be Forgotten and the Right to Data Portability.

30 THE TIMESCALE FOR RESPONDING TO A SUBJECT ACCESS REQUEST IS REDUCING

SUBJECT ACCESS REQUESTS

The timescale for responding to a subject access request has been reduced from 40 to 30 days.

In order to comply with the GDPR you must identify the areas at risk and determine how you will prioritise and manage the rights of the data subject. A good starting point is to understand what personal data you hold, when and how you transfer that data.

Ensure you have robust controls to identify, investigate and escalate any incidents.

It is important to keep up-to-date with the ICO guidance to consider how the GDPR affects you and your organisation.

We welcome any questions you may have in relation to our framework.

Please send your queries to claims@examworks-is.co.uk.

ExamWorks Investigation Services Limited
P.O Box 2157, Bolton, BL6 9BN.
0333 600 1660 | www.examworks-is.co.uk

ExamWorks
Investigation Services

GDPR - DISPELLING THE MYTHS

MYTH **GDPR will become irrelevant to British businesses once the UK leaves the European Union.**

FACT The UK government has confirmed that the UK's decision to leave the EU will not affect the introduction of the GDPR. All companies operating in the UK who process personal data will be in scope for complying with the regulation.

MYTH **Every business will require a Data Protection Officer.**

FACT Data Protection Officers are to be appointed in the following circumstances:

1. You are a public body.
2. You are a private sector controller whose core activities consist of processing operations that require 'regular and systematic monitoring of data subjects on a large scale'.
3. You are a private sector controller whose core activities consist of processing special categories of personal data (e.g. sensitive personal data under the UK DPA).

MYTH **The risks of heavy fines are over-exaggerated.**

FACT Rules behind the fines are not readily available, however, there is nothing to say these fines will not be enforced to the maximum value.

MYTH **All personal data breaches will need to be reported to the ICO.**

FACT It will be mandatory to report a personal data breach under the GDPR if it is likely to result in a risk to Data Subject's rights and freedoms. So if it is unlikely that there is a risk to Data Subject's rights and freedoms from the breach, you do not need to report it.

MYTH **If my data is encrypted that will make me compliant with security regulations and I don't have to worry.**

FACT Encryption alone may not be sufficient enough. Encryption should be regarded as one of many tools to consider as part of securing and minimising the loss or misuse of data. If you have a number of complementary measures in place this will enhance the overall security of the data.

ExamWorks Investigation Services Limited
P.O Box 2157, Bolton, BL6 9BN.
0333 600 1660 | www.examworks-is.co.uk

ExamWorks
Investigation Services