GDPR Staff Newsletter No 1

June 2018

Introduction

The purpose of this newsletter is to update you regarding the introduction into law of the General Data Protection Regulation as from 25 May 2018.

It is the first of a series of newsletters we will be publishing on the subject.
GDPR standardises the laws relating to the protection the personal information of EU citizens and places specific responsibilities on organisations that stores or processes such data even if they are based outside the EU.

The penalties that can be imposed on employers that breach GDPR include fines of up to €20 million or 4% of turnover, whichever is the greater.

What is personal information?

The following diagram shows the main categories of personal information.
This data includes:

- Bank account/Credit cards
- Contact details including e-mail addresses and telephone numbers
- Passports
- Driving licences
- Payroll details
- Date of birth
- Gender
- Ethnicity
- Disability
- Health/Medical conditions
- Political beliefs
- Sexual orientation
- Disciplinary, counselling and attendance records

As an employer we do not hold or process information regarding some of these categories but it is possible that other organisations such as Facebook, LinkedIn or even Amazon do.

What information can we lawfully hold?

Below is a list detailing the reasons under which we are allowed to hold personal data as from 25th May.

We have been reviewing our records to determine if any falls outside these categories.
If any data does fall outside these categories then, as a matter of priority, we are making sure that it is deleted or destroyed before 25th May.

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Processing of sensitive category data;

a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes

b) Is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

c) Is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards e.g. health and safety/union

e) Processing relates to personal data which are manifestly made public by the data subject

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) Processing is necessary for reasons of substantial public interest,

h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment

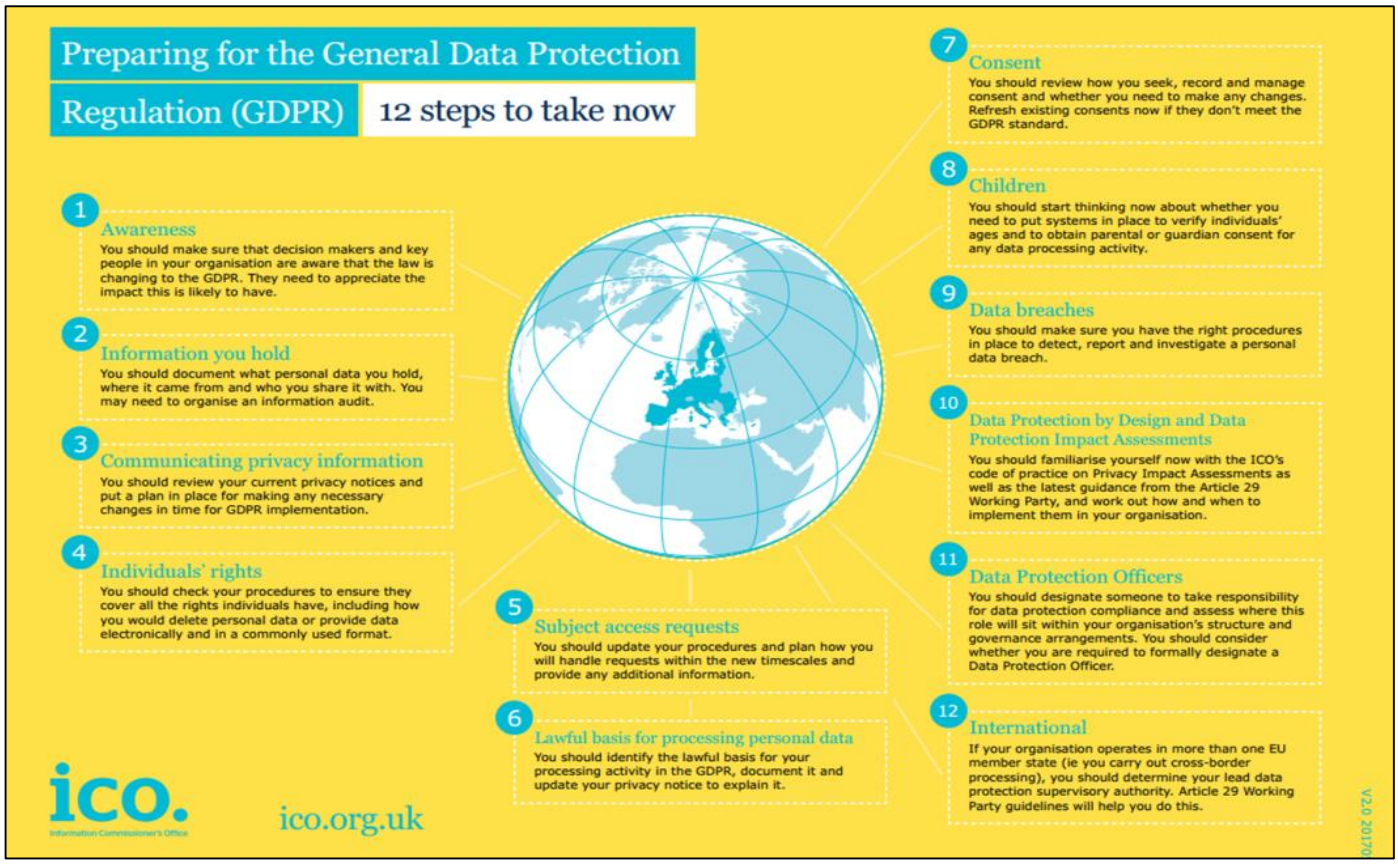
i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health

j) Processing is necessary for archiving

What steps are we taking information to ensure compliance?

GDPR will be policed by the ICO (Information Commissioner's Office) which is contactable via their website www://ico.org.uk

In background we have been working through the ICO's 12 Step approach in preparation for the new legislation.



Over the next few weeks we will be issuing further newsletters that will update you on our progress and hopefully answer the majority of your concerns and any questions you may wish to ask.

GDPR represents a major change for all organisations including our own and as such I would ask for your patience.

If there are any specific questions following the publication of the series of newsletters then please feel free to contact our (Data Protection Officer) on our head office number : 01785 282501