

# Legislation Outlook

September 2017

Tailored updates to legislation are automatically delivered direct into your [Activ Comply](#) system as they come into effect so you can be confident that you're always up to date.

This monthly legislation briefing is a supplement to your Activ Comply service to help you to plan ahead for maintenance of your ISO 14001, OHSAS 18001, ISO 50001 and ISO 27001 systems. In addition to giving you advance warning about important legislation that will affect your compliance with the standards, we'll provide you with news, newly-published guidance and government consultations that you might find useful, as well as any other significant legislation beyond the scope of the standards listed that we think may have a potential impact on your organisation. Unlike other services, we only report items of value: we don't waste your time reporting an increase of administrative fees or changes that will only affect enforcement agencies.

This month has been relatively quiet in terms of new legislation but expect more next month as October is traditionally a busy month. We continue our **GDPR Focus** to help you prepare for the new General Data Protection Regulations. The focus this month is on the distinction between a controller and a processor of personal data, and what that will mean for you.

## Upcoming Standard-Related Legislation

---

### ISO 14001

#### **Regulation (EU) 2017/1369 setting a framework for energy labelling**

This Regulation specifies the requirements for the labelling of energy-related products and the provision of standard product information regarding energy efficiency. Parts of this Regulation came into force in August but those provisions are identical to the obligations already in force under the *Energy Information Regulations 2011*. The Regulation also contains a new obligation requiring suppliers of energy-related products to enter energy information on a product database before they are placed on the EU market; this provision is scheduled to come into force on 1 January 2019.

### OHSAS 18001

#### **Health and Safety (First-Aid) (Amendment) Regulations (Northern Ireland) 2017**

These Regulations come into force in Northern Ireland on 31 October 2017 and remove the requirement for the Health and Safety Executive for Northern Ireland to approve the training and qualification of appointed first-aid personnel.

### ISO 27001

#### **Data Protection Bill 2017**

The Government has announced that this Bill will be published in September 2017 to bring the UK's law into line with the EU's new data protection regulation (the GDPR) and replace existing data protection legislation on both corporate data and data processing by law enforcement agencies. The details of this Bill and when it will come into force are not yet public; we will update you in next month's briefing.

#### **Investigatory Powers Act 2016 (Consequential Amendments and Saving Provisions) Regulations 2017**

These Regulations come into force on 11 September 2017 and transfer functions relating to the supervision of investigatory powers to the Investigatory Powers Commissioner from the, now abolished, Interception of Communications Commissioner, the Intelligence Services Commissioner, the Chief Surveillance Commissioner and other Surveillance Commissioners, and the Scottish Chief Surveillance Commissioner and other Scottish Surveillance Commissioners.

## News

### Preparations Urged for ESOS Phase 2

The important part of the second compliance period for the Energy Savings Opportunity Scheme will get underway shortly. From 31 December 2017, large undertakings who are not ISO 50001 compliant will be able to start the year-long process of measuring their total energy consumption as required by the *Energy Savings Opportunity Scheme Regulations 2014*. Organisations are being urged to act early to minimise disruption, avoid enforcement action and unlock the financial savings brought by greater energy efficiency.

### Lowest Ever Construction Fatality Figures Released by HSE

Provisional annual data for work-related fatal accidents between April 2016 and March 2017 shows 30 fatal injuries to construction workers were recorded, the lowest year on record for the sector. Total deaths have also dropped to 137, the second lowest year on record.

## Guidance

The Environment Agency has published a Technical Guidance Note [here](#) to aid anyone seeking general guidance on the **monitoring of stack emissions to air**. It also contains an index of monitoring techniques and methods designed to help the user to find a solution to a monitoring problem or query.

## Consultations

The Department for Digital, Culture, Media and Sport has launched a public consultation [here](#) about Government plans to **boost network and information security and reduce the risk of cyber-attacks in the UK**.

The Department for Transport, Office for Low Emission Vehicles and Innovate UK have jointly launched a consultation [here](#) about a proposal to **establish low emission light commercial vehicles as an alternative to diesel-powered vans** by allowing category B (car) licence holders to drive a slightly heavier vehicle, if it is powered by a low emission technology.

## GDPR Focus: Controller vs Processor

Are you ready for the **General Data Protection Regulation**? The GDPR comes into force in May 2018, so there is now less than a year to prepare for the new data protection requirements. This month we focus on the important distinction between a **controller** and a **processor** of personal data.

A **controller** is the organisation that determines the purposes and the manner of processing personal data, i.e. they exercise overall control over the 'why' and the 'how' of a data processing activity.

A **processor** is an organisation that processes personal data on behalf of a **controller**.

The GDPR contains distinct obligations for controllers and processors. Under the *Data Protection Act 1998* a processor's obligations were confined to the terms of their service contract with their controller. Under the GDPR, a processor will have direct data protection obligations. In particular, a processor must:

- implement technical and organisational measures to ensure an appropriate level of security for the processing activity; and
- inform the controller without undue delay of any personal data breaches.

In most situations, it will be clear whether you are acting as a controller or a processor.

Bear in mind that most organisations are likely to have controller responsibilities for personal data held for internal purposes, such as their employees' records. If you are a processor, you must be able to distinguish between your 'own' data (for which you are the controller) and the data you process on behalf of a controller (for which you are the processor), so that you can determine what your data protection obligations are in each case.

More on the GDPR next month!

### Like to know more?

0333 301 9003  
legal@myactiv.co.uk  
www.activcomply.co.uk

### Watch the video

[Click here](#)