

Legislation Outlook

November 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.

October saw very little new legislation published. Our regular **GDPR Focus** item, designed to help you prepare for the new General Data Protection Regulation coming into force next May, looks at the new rules for record keeping.

Upcoming Standard-Related Legislation

ISO 14001

Regulation (EU) 2017/1915 prohibiting the introduction into the Union of specimens of certain species of wild fauna and flowers

This [Regulation](#) comes into force on 9 November 2017 and adds 11 species to the list of endangered species whose introduction into the EU are prohibited. The species are:

Macaca fascicularis from Laos;

Kinyongia fischeri and *Kinyongia tavetana* from Tanzania;

Triceros quadricornis from Cameroon;

Hippocampus algiricus from Guinea and Senegal;

Ornithoptera priamus from Solomon Islands (wild and ranched specimens)

Pandinus imperator (ranched specimens) from Ghana; and

Phelsuma borai, *Phelsuma gouldi*, *Phelsuma hoeschi* and *Phelsuma ravenala* from Madagascar.

The Regulation also removes the prohibition on the introduction into the EU of a large number of species which are no longer considered endangered. If your organisation imports flora or fauna into the EU you should check the Annex to the Regulation to see whether any of these changes will affect your business activities

OHSAS 18001

Ionising Radiation Regulations

The Health and Safety Executive has announced that new Ionising Radiation Regulations are likely to replace the Ionising Radiations Regulations 1999 in the New Year. The new Regulations will apply to workplaces where radioactive substances and electrical equipment emitting ionising radiation are used. Proposed changes put forward by the HSE are a reduction in the dose limit for exposure to the lens of the eye and a new three-tiered risk-based system of regulatory control. We will provide further details on these new Regulations when they are published.

News

New ISO 45001 standard likely launched to be launched in early 2018

The working group developing ISO 45001 has met for what is anticipated to be the final time in the development of the occupational health and safety management system standard. The standard is now likely to go to a final draft before publication in March next year, after the working group determined that amendments to the current draft were required due to the large number of comments submitted to an earlier public consultation. However, there remains a small possibility that the standard could be published this year if the amendments are not found to be "technical" by the chair of the working group or the ISO central secretariat.

HSE's construction inspection campaign targets dust exposure

The Health and Safety Executive has announced that the second phase of their targeted inspection initiative will focus on the control of harmful dusts, including respirable silica from concrete, brick and stone, asbestos and wood dust. The HSE aims to use this campaign to ensure that the construction industry manages harmful dust effectively by the use of the right design, equipment and training.

Guidance

The [2018 amendments to the Domestic Building Services Compliance Guide - 2013 edition](#) have been published by the Department for Communities and Local Government. The guidance comes into effect from 6 April 2018 and introduces revised standards for when gas-fired and oil-fired boilers are installed or replaced in existing dwellings.

[Circular 01/2017: Building \(Amendment\) Regulations 2017](#) has been published by the Department for Communities and Local Government to explain changes to building regulations concerning self-certification schemes that allow competent persons to self-certify certain types of building work.

Consultations

The EU Commission has launched a public consultation to assess whether the Batteries Directive (Directive 2006/66/EC, implemented in the UK by the **Batteries and Accumulators (Placing on the Market) Regulations 2008** and the **Waste Batteries and Accumulators Regulations 2009**) has met its objectives and contributes to the general objectives of EU environmental policy. The consultation is available [here](#).

GDPR Focus: Record Keeping

This month we focus on the new **record keeping** requirements in the GDPR. Under the GDPR, any organisation with 250 or more employees will have to maintain a written record of personal data processing activities for which it acts as a controller or a processor.

Article 30 of the GDPR specifies that the records kept by a **controller** must contain:

- the name and contact details of the organisation and, where applicable, the Data Protection Officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- where applicable, the categories of any recipients to whom the personal data have been or will be transferred;
- where applicable, details of transfers of personal data outside the EU and their safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the security measures in place to protect the personal data.

There are similar requirements for **processors**, whose records must contain:

- the name and contact details of the organisation and, where applicable, the Data Protection Officer;
- the name and contact details of the controller on behalf of whom the organisation is processing the personal data;
- the categories of processing carried out on behalf of each controller;
- where applicable, details of transfers of personal data outside the EU and their safeguards; and
- where possible, a general description of the security measures in place to protect the personal data.

Any organisation with under 250 employees should be aware that the record keeping requirements outlined above will also apply to them IF the processing:

- is likely to result in a risk to the rights and freedoms of data subjects (this is defined in Recital 75 of the GDPR as processing which may give rise to any significant economic or social disadvantage, e.g. discrimination, identity theft or damage to the reputation; where data subjects might be deprived of their rights, where personal aspects are evaluated, e.g. performance at work, reliability or behaviour, location or movements, in order to create personal profiles; where personal data of vulnerable people, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects);
- is not occasional (there is no UK guidance available yet as to what is "occasional" processing but Belgium's equivalent of the ICO has provided guidance that processing activities related to employee, client or supplier management would not be considered occasional);

- includes special categories of data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation); or
- includes personal data relating to criminal convictions and offences.

These exceptions, in particular the "occasional" processing exclusion, create an extremely low threshold for an organisation with under 250 employees to reach. In practice, therefore, all organisations, regardless of the number of employees, should comply with the new record keeping obligations in the GDPR.

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](#) to see Activ Comply in action