activcomply
intelligent legal compliance

Legislation Outlook

May 2018

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 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 an impact on your organisation. Unlike other services, we only report items of value: we don't waste your time on items such as an increase of administrative fees or changes that only affect enforcement agencies.

When legislative changes are announced with short notice (<1 month) they are not reported here. All changes are automatically delivered direct into your Activ Comply system as they come into effect so you can be confident that you are always 100% up to date.

April and May are traditionally busy months in terms of new legislation being published and 2018 has been no different. As usual, we have provided a summary of legislation that won't come into force immediately, as well as our ongoing GDPR Focus, which this month concentrates on transfers of personal data outside the European Union.

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

Upcoming Standard-Related Legislation

ISO 14001

Motor Vehicles (Construction and Use) (Amendment) Regulations (Northern Ireland) 2018

These Regulations come into force on 20 May 2018 and amend the Motor Vehicles (Construction and Use) Regulations (Northern Ireland) 1999 to lower the permissible coefficient of absorption of the exhaust emissions from diesel-engined vehicles first used on or after 1 January 2014. It also provides new braking efficiencies for the primary and secondary braking systems of motor tractors driven at more than 40km/h.

OHSAS 18001

Regulation (EU) 2018/605 amending Annex II to Regulation (EC) No 1107/2009 by setting out scientific criteria for the determination of endocrine disrupting properties

This Regulation comes into effect on 20 October 2018 and amends Regulation (EC) No 1107/2009 concerning the placing of plant protection products on the market. In order to reflect the current state of scientific and technical knowledge, the Regulation has updated the criteria for determining whether active substances, safeners and synergists in plant protection products possess endocrine disrupting properties that can have an adverse effect on humans and other non-target organisms. Producers of active substances, safeners and synergists used in plant protection products will need to implement the new four-part test for identifying substances with endocrine disrupting properties before 20 October.

ISO 27001

Network and Information Systems Regulations 2018

These Regulations come into force on 10 May 2018 to implement a national framework for the security of network and information systems in the United Kingdom. It places obligations on operators of essential services (OES). Essential services are defined in the Regulations as undertakings carrying out specified tasks in the electricity, oil, gas, air transport, water transport, rail transport, road transport, drinking water and digital infrastructure industries. An OES will have to comply with the following obligations:

(i) take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies;
(ii) take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services; and
(iii) notify the designated competent authority for the industry about any incident which has a significant impact on the continuity of the essential service which that OES provides.

Remember: short-notice changes to legislation are not reported in this briefing; all changes are delivered direct into your Activ Comply system as they come into effect.

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

News

GDPR!

More than two years after it was first published, the EU's new data protection regime will come fully into effect on 25 May. There are a number of differences to the current legislation, the Data Protection Act 1998, including tougher sanctions for non-compliance, more stringent consent requirements, new special categories of personal data, enhanced privacy notices and record-keeping requirements, the introduction of data protection by design and data protection by default, and a new requirement to designate a Data Protection Officers for certain organisations. A summary of all these changes and more is available here.

Invite someone else to subscribe to this Briefing

Consultations

Marine plan for Northern Ireland

The Department of Agriculture, Environment and Rural affairs has launched a consultation on the proposed Marine Plan for Northern Ireland, which will be used by public authorities in taking decisions that affect the marine area, including authorisation or enforcement decisions.

Environmental impact of machine tools and welding equipment

The European Union has launched a consultation on potential measures for regulating the environmental impact of machine tools and welding equipment.

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

GDPR Focus: Transfers of Data

This month we look at the rules concerning transfers of data outside the EU. The rules have not changed drastically under the GDPR in comparison to the existing Data Protection Act 1998; the basic principle is still that transferring personal data for processing outside the EEA is prohibited, with permissible exceptions. Some of the detail has changed, the most significant being the brand new "Binding Corporate Rules" exception.

Under the GDPR transfers outside the EEA are allowed in the following circumstances:

(i) Where the Commission as decided that the country concerned provides an adequate level of protection. Currently, the only countries this applies to are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Companies in the United States who are signed up to Privacy Shield are also regarded as adequate. You can check whether a US company has signed up to Privacy Shield by visiting www.privacyshield.gov.

(ii) Where "standard data protection clauses" (also known as "model clauses") are in place with the recipient of the personal data. These are template contracts that are approved by the EU Commission. There are currently three model contracts: two governing transfers of personal data between controllers and the other governing transfers of data between a controller and a processor. More details are available on the Commission's website.

(iii) Where Binding Corporate Rules (BCR) allow the transfer of personal data within multinational corporate groups. This is a new concept in the GDPR, and allows global companies to move personal data much more freely and flexibly within their group structure, provided that their BCR are approved by the Information Commissioner's Office.

(iv) Where none of the above options apply, you can seek to rely on one of the six derogations available. These are:

- Consent – the data subject has explicitly consented to the transfer after being informed of the possible risks of the transfer due to the lack of an adequacy decision and appropriate safeguards.
- Contractual performance – in the case of a contract between the exporter of the personal data and the data subject, the transfer can be carried out where it is necessary for the performance of the contract or any pre-contractual measures taken at the request of the data subject. In the case of a contract between the exporter and someone other than the data subject, the contract must be entered into either at the data subject's request or in their interest, and again the transfer must be necessary for the performance of the contract.
- Substantial public interest –the transfer must be necessary for important reasons of public interest, such as crime prevention or national security.
- Legal claims – the transfer of personal data will be allowed where it is necessary for the establishment, exercise or defence of legal claims.
- Vital interests – this derogation allows the transfer of personal data in matters of life or death, for example where a data subject's medical records are transferred following a serious illness or accident abroad.
- Public registers – this final derogation allows personal data that is available on public registers, e.g. company directors, to be transferred outside the EEA.

(v) Finally, and as a last resort, transfers outside the EEA are allowed where they are not repetitive, concern only a limited number of data subjects, are necessary for the purposes of compelling legitimate interests pursued by the transferor (and those

compelling legitimate interests are not overridden by the interests or rights and freedoms of the data subject), and the transferor has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. On top of that, the transferor must also notify the ICO and the data subject of the transfer.

If you want to review previous items in the GDPR Focus series, you can do this in your Activ system on the **Legislation Outlook** tab. If you receive this briefing by e-mail, contact us to request previous months' issues.

Activ is compliant with the GDPR

In our relationship with you, we are acting as the processor of the personal data you hold within your Activ system and you are the controller. As your organisation works towards compliance with the GDPR you will require certain information from us. Please direct any requests for information relating to our compliance with the GDPR to gdpr@myactiv.co.uk.

Do you need help with GDPR compliance? Through our consultancy division, ISO in a Box™, we have been leading the way in simple, assured compliance practices for nearly 20 years.

Visit our consultancy **website** for GDPR resources and more information on our cost-effective support packages to deal with GDPR, or **contact** our friendly team.

GDPR is covered in Activ Comply

The requirements of the GDPR are available in your Activ Comply system as a supplementary 'standard' at no extra cost.

Click here for further information and contact us to switch this feature on for you.

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