activcomply
intelligent legal compliance

Legislation Outlook

October 2021

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 45001, 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 will potentially impact your organisation. Unlike other services, we only report items of value: we don't waste your time on items such as an increase in 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.

Another quiet month for standard-related legislation. However, the Government has released its proposals for its replacement to GDPR, see the Focus section at the end of the Outlook for more information on the proposed data protection reforms.

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

Upcoming Standard-Related Legislation

There is no upcoming standard-relating legislation to report this month.

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.

News

IPCC Warns of Accelerating Global Warming

The UN's Intergovernmental Panel on Climate Change has published a report warning that the rise in global temperatures will exceed 1.5°C above pre-industrial levels during the next 20 years, around a decade earlier than previously thought. At the same time, an Ipsos MORI poll has found that the UK public are more concerned about the environment than at any in the last thirty years. Business is likely to face increased pressure from both government and consumers to be able to present their 'green' credentials effectively, potentially increasing the significance of ISO 14001 certification.

Fatalities at Work Increase by 28%

The Health and Safety Executive has reported that work-related accidents resulted in 142 deaths in the year ending 31 March 2021, a rise of 31 deaths from the previous year. However, the number of deaths in the previous year was low in comparison to other recent years, and in statistical terms the number of fatalities has remained broadly level in recent years – the average annual fatality rate for the last five years is 136.

Consultations

Groundwater and Surface Water Discharge Activities

The Department for Environment, Food & Rural Affairs has launched a consultation seeking views on plans to amend the Environmental Permitting (England and Wales) Regulations 2016 as they apply to groundwater activities and some related surface water discharge activities. The proposed amendments aim to:

- improve the hierarchy of regulatory controls for groundwater activities;
- provide controls for a greater range of potential pollutants; and
- improve existing control measures for protecting groundwater from site-based activities.

The consultation closes on 22 December 2021.

Data Protection

The Department for Digital, Culture, Media & Sport has issued a consultation on proposals to reform the UK's data protection regime. See the Focus section below for more information on this. The consultation closes on 19 November 2021.

Focus: Data Protection Reform Proposals

The Government has published extensive proposals for reform of the data protection regime in its document Data: A New Direction in probably the biggest change to any of the UK's regulatory regimes since its withdrawal from the European Union.

The government proposals build on the key elements of the GDPR, including its data processing principles, data rights, and supervision and enforcement mechanism, but also looks to remove unnecessary burdens on business and deliver better outcomes.

The Consultation focuses on five areas:

1. Reducing barriers to responsible innovation

Proposals in this area look to:

- Consolidate and simplify safeguards and the lawful grounds for processing personal data for research purposes;
- Provide greater clarity of when personal data can be re-used for 'further processing' without having to provide additional information to the data subject;
- Create a limited, exhaustive list of legitimate interests as a lawful ground for processing so that organisations whose processing is covered by the list aren't required assess the impact of their processing on the rights and freedoms of data subjects or rely unnecessarily on consent;
- Introduce AI specific provisions, including:
    - the concept of 'fair use' to AI related processing;
    - allowing the processing of personal data, including sensitive personal data for the purposes of ensuring bis monitoring, detection and correction in AI systems; and
    - clarifying how data subject rights in relation to automated decision making and subject access request will work in relation to AI;
- Create a clear test for when data will be regarded as anonymous.

2. Reducing burdens on business and delivering better outcomes for people

Proposals in this area are likely to have a significant impact on organisation's data protection compliance activities through the implementation of a more flexible and risk-based accountability framework - the **Privacy Management Program ('PMP')**.

The requirements for a PMP are set out in paragraph 156 of the consultation, but are also reproduced here for convenience. The PMP must include the appropriate policies and processes for the protection of personal information and, specifically, cover:

- The roles and responsibilities within the organisation in relation to personal data protection, including who is designated as the responsible individual(s) for the privacy management programme and overseeing the organisation's data protection compliance. The designated individual(s) will also be responsible for representing the organisation to the ICO and data subjects where necessary. The legislation would not prescribe the specific requirements needed for the role(s) and an organisation would have discretion over appointments, including by being able to determine the appropriate skills, qualifications and position needed for the role(s), taking account of the volume and sensitivity of the personal information under its control, and the type(s) of data processing it carries out.
- Evidence that oversight and support from senior management, and appropriate reporting mechanisms to senior management, are in place, and how the organisation ensures its staff understand key data protection obligations, policies and processes.
- Measures which assist the designated responsible individual(s) for structuring an appropriate privacy management programme and demonstrate the organisation is compliant with data protection legislation. These include:
    - Personal data inventories which describe and explain what data is held, where it is held, why it has been collected and how sensitive it is;
    - Internal policies that address the organisation's obligations under the data protection legislation;
    - Risk assessment tools for the identification, assessment and mitigation of privacy risks across the organisation;
    - Procedures for communicating with data subjects about their data protection rights and the organisation's policies and processes under a privacy management programme;
    - How requests for information and complaints are received and dealt with; and
    - Procedures for handling breaches.

Other proposals in this area of the consultation include:

- Removal of the requirement for certain organisations to designate a data protection officer. The proposed alternative is to require an organisation to designate a suitable individual, or individuals, to be responsible for the PMP and for overseeing the organisation's data protection compliance;
- Removal of the requirement for organisations to undertake a data protection impact assessment, so that organisations may adopt different approaches to identify and minimise data protection risks that better reflect their specific circumstances, and removal of the requirement for prior consultation with the Information Commissioner's Office in relation to high-risk processing;
- Removal of most record keeping requirements. A PMP would still require certain records be kept but organisations will have more flexibility about how to do this in a way that reflects the volume and sensitivity of the personal information they handle, and the type(s) of data processing they carry out;

- Increasing the threshold for reporting a data breach to the ICO so that organisations only need to report a breach where there is a material risk (rather than any risk) to individuals;
- Introduce a fee regime for subject access requests to reduce their number;
- Permit organisations to use analytics cookies and similar technologies without the user's consent;
- Implementing a more flexible and risk-based accountability framework which is based on privacy management programmes; and
- Extend the soft opt-in to electronic communications containing direct marketing from organisations other than businesses where they have previously formed a relationship with the person.

3. Boosting trade and reducing barriers to data flow

Proposals in this section of the consultation will be particularly important for organisations that transfer personal data outside the United Kingdom. The proposals include:

- An outline of the Government's procedure for making adequacy assessments of other jurisdictions.
- Ensuring that the suite of data transfer mechanisms other than adequacy decisions available to UK organisations (e.g. binding corporate rules and standard contractual clauses) is clear, flexible and provides the necessary protections for personal data.
- Exempting 'reverse transfers' from the scope of the UK international transfer regime.
- Modifying the framework for certification schemes to provide for a more globally interoperable market-driven system that better supports the use of certifications as an alternative transfer mechanism; and
- Increasing the flexibility for the use of derogations for transfers without appropriate safeguards by making explicit that repetitive use of derogations is permitted.

4. Delivering better public services

Proposals relating to the processing of personal data by public authorities are not as significant as the proposals in other areas, but there are still a couple of noteworthy changes proposed:

- The introduction of compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data; and
- Adding new situations, or amending existing situations, in which sensitive personal data can be processed for reasons of 'substantial public interest'.

5. Reform of the Information Commissioner's Office

Whilst there are many proposals for reform to the ICO, much of it relates to administrative and governance changes that will not be noticed by external parties. In relation to proposals that may affect organisations, there are some relatively minor proposals in relation to the ICO's enforcement power, such as the power to compel witnesses to answer questions at interview in the course of an investigation and amending the statutory deadline for the ICO to issue a final penalty notice following a Notice of Intent from 6 months to 12 months, but there is little else of note.

Conclusion

It is important to restate that this is a consultation and that the proposals may be implemented differently or even not be implemented at all. However, it is an indicator of the direction the Government are looking to take in relation to data protection, and organisations (particularly those that hold ISO 27001 certification) should be prepared for significant changes in the near future.

Invite someone else to subscribe to this Briefing

Like to know more?

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

Take control of your ISO management system

Do you know about Activ's other ISO management modules, designed by ISO experts to simplify management system maintenance?

Click here for more information