



Legislation Outlook

November 2022



This monthly legislation briefing is a **supplement** to our BAB Activ Comply service to help you to **plan ahead** for the maintenance of your ISO 14001, ISO 45001, ISO 50001, ISO 22301 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 directly into the **BAB 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, but this month has seen the publication of a new version of ISO 27001 - see below for more information on the changes to the popular information security standard.

Upcoming Standard-Related Legislation

ISO 14001/ISO 50001

Building etc. (Amendment) (England) (No. 2) Regulations 2022

These [Regulations](#) come into force on 29 March 2023. They amend the Building Regulations 2010 as they apply in Wales to extend the scope of paragraph L2 of Schedule 1 (which requires that any on-site electricity generation must be appropriately sized for the site and available infrastructure; have effective controls, and must be commissioned by testing and adjusting as necessary to ensure that it produces the maximum electricity that is reasonable in the circumstances) to non-domestic premises.

ISO 27001

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)

This [EU Regulation](#) will affect the EU operations of 'online gatekeepers' when it comes into force on 2 May 2023. Companies are considered gatekeepers if:

- they provide a core platform service (i.e. online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communications services, operating systems, web browsers, virtual assistants, cloud computing services, and online advertising services) in at least three EU countries with at least 45 million monthly end users and at least 10 000 business users; and
- they have a significant impact on the EU market (this is presumed to be satisfied by having an annual turnover of €7.5 billion in the last three years, or where its average market capitalisation or a valuation of €75 billion).

The new law aims to level the playing field between smaller and larger digital platforms to ensure a competitive and fair digital sector. To achieve this, Gatekeepers will be prohibited from:

- ranking their own products or services higher than those of others;
- preventing developers from using third-party payment platforms for app sales;
- processing users' personal data for targeted advertising, unless consent is granted;
- establishing unfair conditions for business users;
- pre-installing certain software applications or preventing users from easily un-installing them; and
- restricting business users of platforms.

Gatekeepers will also be obliged to:

- offer more choices, such as the choice of certain software on a user's operating system;
- ensure that unsubscribing from core platform services is as easy as subscribing;
- provide information on the number of users that visit their platforms to determine whether the platform can be identified as a gatekeeper;
- give business users access to their marketing or advertising performance data on the platform;
- inform the European Commission of their acquisitions and mergers; and
- ensure that the basic functionalities of instant messaging services are interoperable (i.e. enable users to exchange messages, and send voice messages or files).

Gatekeepers who do not comply with the new rules will potentially face fines of up to 20% of global turnover.

ISO 27001 Internal Auditor Training Course

Hone your internal auditing skills of ISO 27001 with our great course!

[Find Out More](#)

News

New Version of ISO 27001 Launched

The International Organization Standardisation has published an updated version of ISO/IEC 27001, now titled 'Information Security, Cybersecurity and Privacy Protection' to recognise the increased importance of cyber resilience to organisations. The most significant change to the Standard is to Annex A where, in order to align with the latest version of ISO 27002 which was published earlier this year, a number of controls have been merged and renamed – this has resulted in a decrease in the number of controls from 114 to 93. The controls have also now been organised into four categories – organisational controls, people controls, physical controls and technological controls.

It is expected that certification bodies will be able to assess against the new standard from some time in the first half of 2023, but the exact timing is dependent on UKAS which has yet to publish information on when the required transition assessments for certification bodies will take place.

ISO 27001 Awareness Training

Grow your knowledge of how
ISO 27001 can help you and
your company!

[Find Out More](#)



Consultations

Employee Monitoring

The Information Commissioner's Office is producing topic-specific guidance on employment practices and data protection, which aims to provide practical guidance about monitoring workers in line with data protection legislation and aims to promote good practice.

Before drafting such guidance they have opened a [consultation](#) and are looking for input from relevant stakeholders including:

- employers;
- professional associations;
- those representing the interests of staff;
- recruitment agencies;
- employment dispute resolution bodies;
- workers;
- volunteers;
- employees; and
- suppliers of employment technology solutions.

This consultation closes on 11 January 2023.

Privacy-Enhancing Technologies

The Information Commissioner's Office has opened a [consultation](#) calling for views on its updated draft guidance on anonymisation, pseudonymisation and privacy-enhancing technologies.

This guidance will be published as a single document, incorporating the following updated chapters:

- Introduction to anonymisation;
- identifiability;
- pseudonymisation; and
- accountability and governance.

This consultation closes on 31 December 2022

Legislation Outlook




USE ACTIV TO HELP YOU
COMPLY WITH DATA
PROTECTION (GDPR)
REQUIREMENTS!

[BOOK A DEMO](#)

ACTIV SECURE HELPS
YOU MONITOR AND
MANAGE INFORMATION
SECURITY RISKS.

[Book a Demo](#)



For the best
help with ISO
27001,
use
ActivSecure

[Invite someone else to subscribe to this Briefing](#)



Would you like to book a free BAB
Activ Comply demo?

[Click here to book your free demo](#)

Looking for an ISO or business
training course?

[Click here to view all our training
courses](#)