Authorised Corporate Service Provider: compliance requirements

General Features



29 September 2025

Tax advisers must comply with specific record-keeping and verification processes to enhance corporate transparency and reduce fraud risks.

Key Points

What is the issue?

The Authorised Corporate Service Provider (ACSP) regime requires third-party agents such as tax advisers who file documents at Companies House to register as ACSPs and verify client identities. This regime aims to enhance transparency and compliance in corporate filings.

What does it mean for me?

CIOT and ATT members filing on behalf of clients must register as ACSPs to continue submitting documentation to Companies House. ACSPs must verify client identities before filing and cannot file without completed verification.

What can I take away?

ACSPs must keep their own registration details current, including AML supervisor changes, senior contact updates, and address changes. Failure to update within 14 days can lead to fines, suspension or cessation of ACSP status, preventing clients' filings and causing reputational harm.

The Authorised Corporate Service Provider (ACSP) regime is now in force. The Economic Crime and Corporate Transparency Act 2023 introduced new registration requirements for third-party businesses and individuals filing information at Companies House and for verifying the identity of directors and people with significant control.

This process is intended to improve the integrity of the Companies Register, aiming to reduce fraud, the use of false identities and 'shell' companies. The ID verification process is intended to enhance trust in those behind companies (including owners, controllers and directors).

Once the filing requirements become mandatory in Spring/Summer 2026, any CIOT or ATT member who will be filing documentation on behalf of their clients (including accounts) at Companies House will need to be registered as an ACSP in order to be able to do so.

However, third parties are able to register their business as an ACSP now, and firms are able to verify the identity of clients on a voluntary basis.

But what does this mean in practice? What are the rules? How do advisers comply with ID verification for ACSP? What does this mean for advisers in terms of risk and what processes do they need to consider implementing in practice?

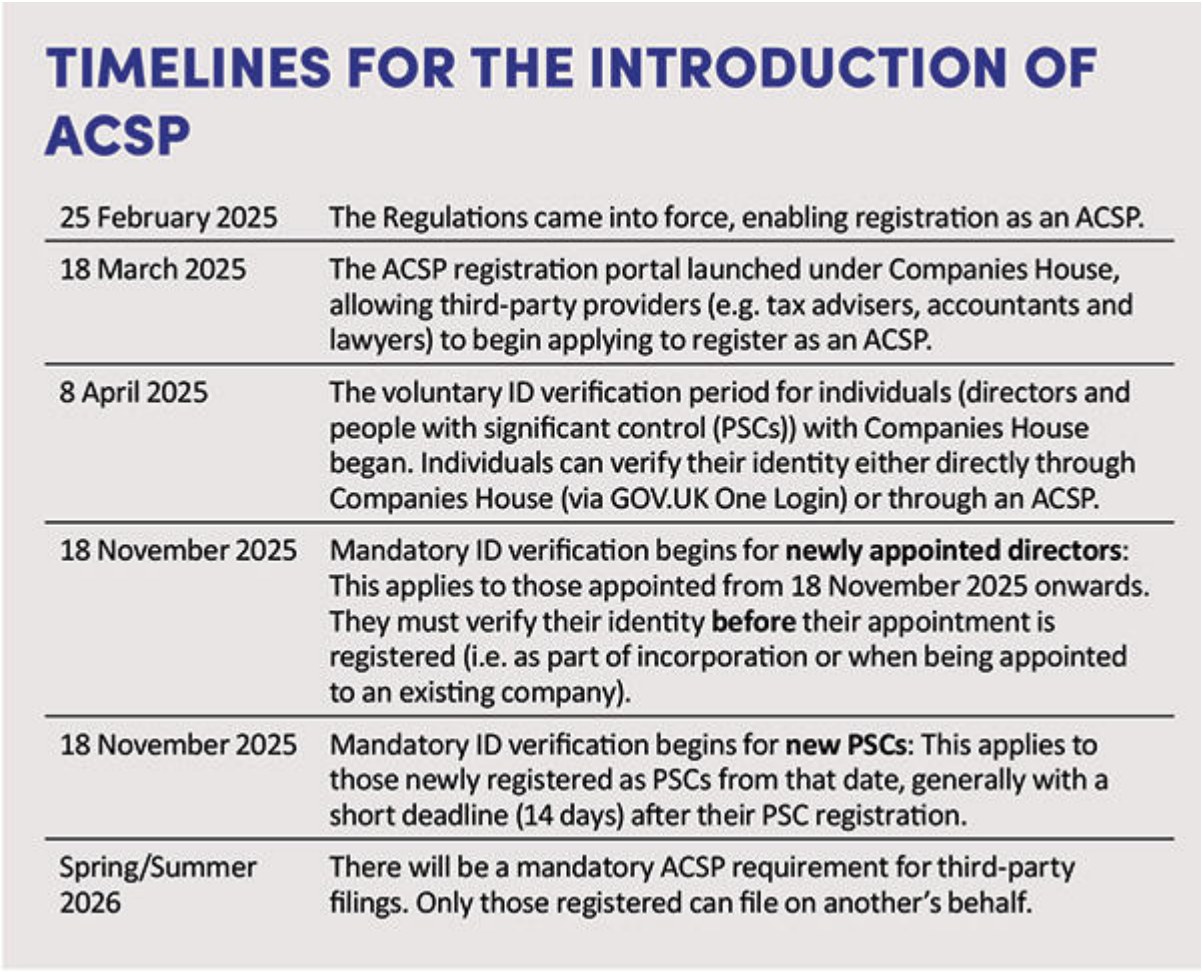
The introduction of ACSP

There has been some confusion over the timelines relating to identity verification and filings. The timeline opposite sets out the schedule for the introduction of ACSP.

However, this timetable relates to mandatory ID verification for newly appointed directors and new PSCs. Because many existing directors and PSCs already hold those roles, there is a 12-month transition period for them starting from 18 November 2025:

- Existing directors must verify their identity by the time that their first confirmation statement due after 18 November 2025 is filed.
- If existing PSCs are also directors of the same company, their deadline generally aligns with the confirmation statement date.
- If they are PSCs but **not** directors, their deadline is related to their birth month (the first day of the month of birth) after 18 November 2025, and they must complete verification within a 14-day window.

Image



TIMELINES FOR THE INTRODUCTION OF ACSP

25 February 2025	The Regulations came into force, enabling registration as an ACSP.
18 March 2025	The ACSP registration portal launched under Companies House, allowing third-party providers (e.g. tax advisers, accountants and lawyers) to begin applying to register as an ACSP.
8 April 2025	The voluntary ID verification period for individuals (directors and people with significant control (PSCs)) with Companies House began. Individuals can verify their identity either directly through Companies House (via GOV.UK One Login) or through an ACSP.
18 November 2025	Mandatory ID verification begins for **newly appointed directors**: This applies to those appointed from 18 November 2025 onwards. They must verify their identity **before** their appointment is registered (i.e. as part of incorporation or when being appointed to an existing company).
18 November 2025	Mandatory ID verification begins for **new PSCs**: This applies to those newly registered as PSCs from that date, generally with a short deadline (14 days) after their PSC registration.
Spring/Summer 2026	There will be a mandatory ACSP requirement for third-party filings. Only those registered can file on another's behalf.

Some key rules

If tax advisers are acting as ACSP, there are some relevant rules that they must be aware of.

ID verification of clients: The role of the ACSP will not only be to file the documentation on behalf of their clients. They must also undertake the ID verification of their clients (or ensure that their clients have done this themselves). The ACSP will not be able to file documentation for their clients if ID verification has not been undertaken.

Record keeping requirements: There is one important change to record keeping requirements. Under usual anti-money laundering (AML) regulations, AML records are kept for **five** years after the client relationship ends. However, for ACSP purposes, the records of client verification must be kept for **seven** years from the request for ID verification. There will need to be a change to the document retention policies and procedures to ensure that practitioners satisfy both obligations.

Updating requirements: There is a positive duty for the ACSP to comply with updating requirements for their own details, with significant consequences if they fail to do so (see below). The ACSP must always be registered with at least one AML supervisory body; and must inform Companies House if the information submitted about the ACSP changes, within 14 days of the change. If requested, the ACSP must also provide information about their filings with Companies House, ID checks, and proof that they are complying with their legal responsibilities.

How does the agent comply with ID verification

There are three ways in which ID verification for ACSP can be carried out under the new regime. There are pros and cons of each, which advisers should consider before deciding which is the most appropriate option for their business.

Ask the client to verify their own identity

Clients can verify their own identity using the GOV.UK One Login service. This service is free and can be completed using a smart phone or by entering ID details online and completing the process in person at a participating Post Office branch.

This may be an attractive option at first sight. However, clients may not expect or want to undertake the process themselves, expecting their adviser to carry out the

process for them. Many clients will also not understand that the process of ID verification is different from the AML process, which must be undertaken by advisers.

If the tax adviser refuses to undertake ID verification (whilst still wanting to undertake AML), tensions may creep into the relationship which will need careful handling, particularly if other advisers are prepared to undertake ID verification for clients.

Identity Document Validation Technology

Identity Document Validation Technology (IDVT) is technology that allows advisers to verify a client's identity remotely using biometric documents (such as passports, driving licences or biometric residence permits) together with facial recognition or liveness checks. The cost is relatively modest, possibly less than £10 per verification, and it should be possible to disburse that cost back to clients.

The IDVT verification should also comply with AML verification requirements and so would not amount to a duplication of cost and process – though as these are different processes, the results need to be stored differently. The adviser will be responsible for the outcome of the IDVT search, so it is important to ensure that it is properly performed and the IDVT provider is credible.

ID verification training

The final option is to send one or more staff members on approved document verification training courses, so that they can verify client documents such as passports and driving licences. It is important to note that merely seeing the documents if you haven't been on the course will not amount to compliance with the regulations.

The cost of the course can be significant and the risk of making errors in the verification are likely to be greater than if using IDVT.

Risks with ID verification

If the ACSP chooses to adopt the manual method of ID verification – training staff to check client documents themselves – there are important risks and practical issues

to consider, and the risk of error is likely to be higher. Primarily, if the person who verifies the documents isn't properly trained, the verification process will not be valid.

The adviser must be able to prove that verification is carried out in line with Companies House requirements. Guidance suggests the while the client doesn't always need to be seen in person, the original documents may need to be physically checked, and scanned copies may not suffice.

If the verifier fails to spot a counterfeit passport or other fraudulent ID, the adviser has technically not complied – even if they acted in good faith. In such a case, regulators are likely to scrutinise what steps the adviser took, and whether they were adequate in the circumstances.

If a client later turns out to have a false identity, the adviser must show a clear audit trail of all verification steps taken. Without such records, it will be difficult to defend the firm's position. Strong internal processes – including training, checklists, escalation procedures and record-keeping – are essential to mitigate this risk.

By contrast, using IDVT provides an automated, standardised process that is easier to evidence and defend. It also creates a digital audit trail of checks performed, such as chip validation, biometric match and fraud detection). Finally, IDVT can support remote verification without requiring clients to present themselves in person. However, deciding which process to use and how to manage that internally will be a decision for each firm, based on their risk and client profile.

Keeping agent information up to date

One issue which advisers registering as ACSPs need to be acutely aware of — and for which they must put in place robust, well-documented processes — relates to an aspect that is rarely discussed: keeping the agent's own information up to date.

To register as an ACSP, a firm must:

- already be supervised under the UK Money Laundering Regulations (AML supervision);
- have a senior member of the firm make the application, using a monitored email address and providing the firm's address;

- ensure that the applicant verifies their own identity (usually via the GOV.UK One Login system); and
- add other members of the firm as users if needed (these users do **not** need to verify their identity individually).

Problems, though, can emerge when there are changes within the firm: the firm changes its AML supervisory body; the senior member who originally made the application retires or resigns; or the firm moves offices or changes its registered details. In many practices, these updates are overlooked. However, under the ACSP regime, failing to act quickly creates serious legal and operational risks.

The official Companies House guidance is clear:

'The agent will be committing an offence if they do not comply with legal requirements. This means the sole trader, or all company directors (or equivalent), could receive a fine or face criminal prosecution.'

Companies House may suspend or cease (revoke) the authorised agent's status. This means that:

- The agent cannot file on behalf of clients or verify identities, and the agent's online account will be closed, and all users will lose access. This could delay transactions, funding or sales. Clients could suffer financial loss and may pursue claims against the adviser.
- Companies House will publish the agent's name, status and date of suspension/cessation, creating reputational damage.
- If necessary, Companies House will contact clients whose identities were verified by the adviser and require re-verification.

Even inadvertent administrative failures (such as missing an email after a partner retires) could cause significant client dissatisfaction and attrition.

In conclusion

Maintaining accurate and up-to-date ACSP information is a business-critical compliance obligation. Firms must treat ACSP updates as seriously as AML obligations – because the consequences of non-compliance can include criminal liability, reputational damage and direct financial harm to both the adviser and their

clients.

© Getty images