What requirements must BPO and IT outsourcing providers meet to be allowed on the European market?

Last updated:
30 June 2025

The rules and regulations for BPO and IT outsourcing are changing rapidly, with a lot of new legislation being introduced. In addition to copyright and data protection requirements, you should understand new legislation related to artificial intelligence, cyber security and corporate sustainability due diligence. In addition, buyers require the presence of a quality management system and environmental and social sustainability practices. You should monitor what standards are important for your product-market combination.

Contents of this page

1. What are the mandatory requirements for BPO and IT outsourcing providers?

Legal requirements are mandatory for companies entering the European outsourcing market. This includes legislation on copyright, general data protection, ePrivacy, artificial intelligence (AI) and cyber security.

You should read the specific rules for your European target market. ePing (a WTO, ITC and UN initiative) provides an overview of country-specific measures that affect trade, which are different from international standards. It also lists contact details for country agents appointed by the World Trade Organisation (WTO). You can subscribe to receive 'ePing alerts' that are relevant to your product or service. Contact Open Trade Gate Sweden if you have specific questions regarding rules and requirements in Sweden and the European Union.

Copyright Directive

Copyright is a type of intellectual property that protects original works of authorship as soon as an author fixes the work in a physical form of expression. Examples of work on which copyright exists are: illustrations, musical compositions, computer programmes, software codes, books, blog posts and much more.

The European Union (EU) has established specific copyright rules to protect computer programs. According to the Directive on the legal protection of computer programs (2009/24/EC), you must make sure not to breach any copyright when placing your computer program on the market. At the same time, your products are also protected against unauthorised reproduction. As an outsourcing provider, however, you often do not have copyright on the work you do for your clients.

In addition, the EU Database Directive (96/9/EC) provides legal protection for databases and consists of two aspects:

- Copyright protection for the creative work in how the materials are selected and arranged; and
- *Sui generis* protection for cases where there has been a large investment in collecting, checking, or presenting the contents of a database.

Tips:

Read more about the legal protection of computer programs.

Check the exact regulations in your European target market. All EU member states have implemented the European Directive in their national legislation. Though this legislation is mostly the same, there may be minor differences.

Be aware of clauses on copyright and infringement (the act of breaking or disobeying a contract) in contracts you sign with European buyers. Clearly agree on how the software may be used and whether there are any limitations or restrictions on its use in the software license agreement.

Read this blog by Cshark about copyright for software development outsourcing. It gives a good overview and provides interesting tips. For more information on copyright when using AI, read the blog on artificial intelligence and copyright by the European Innovation Council and SMEs Executive Agency.

General Data Protection Regulation

The General Data Protection Regulation (GDPR – EU 2016/679) is designed to protect individuals in Europe from privacy and data breaches. It aims to give people more control over their personal data and gives businesses a set of rules to comply with. The GDPR applies to all companies that process the personal data of individuals in Europe, regardless of a company's location. Therefore, it also applies directly to you. Be aware that if your company is located outside the EU and you handle EU citizens' data, you need to appoint a representative within the EU.

Under the GDPR, any company or individual that processes data from European consumers is responsible for protecting that data. Examples of protected personal data are names, email addresses, bank details, social media content, photos and IP addresses. When you transfer personal data outside the EU, you must still protect the data according to the GDPR.

Figure 1: GDPR-protected consumer rights

Source: Globally Cool

Important consumer rights protected by the GDPR include, but are not limited to:

- Consent (approval): Consumers must explicitly agree to the use of their data by opting in, consent must be easy to withdraw, and requests to use data must be specific and in language that is easy to understand;
- Right to access: Consumers have the right to know if companies will process their personal data, where they will do so and for what purpose;
- Right to be forgotten: Consumers have the right to have their personal data removed and to stop further processing and sharing of their data; and
- Privacy by design: Data protection must be included from the start of every project or contract. The use of data must be minimised and access to it limited.

In July 2023, the European Commission made a proposal to improve GDPR enforcement. The proposal aims to make enforcement procedures work better and faster in cases where personal data is processed in multiple countries. The proposal suggests standardising the procedural rights of all parties, improving cooperation between supervisory authorities and clearly explaining how to resolve disputes under the GDPR. The European Parliament adopted its position in April 2024, and the Council followed in June 2024. The amendments are still being negotiated and could change in the coming years.

Tips:

- If you use/process personal data, learn about the GDPR's European data protection rules and key principles to understand what is allowed and what is not. For the United Kingdom (UK), check the UK's GDPR guidance and resources.
- Check if you currently meet GDPR standards. What data do you have, where and why? Have you or your client obtained explicit consent to use it for this specific purpose?
- Set up clear consent request forms and privacy policies explaining how you process personal data. This way, your clients (and their customers) will be fully informed. Read these best practices on creating GDPR-compliant privacy notices (with examples).
- Use IDC's GDPR Readiness Assessment to find out how compliant you are and what you need to improve.
- Stay updated on amendments to the GDPR. Although the main principles of the GDPR will remain the same (i.e. the focus is on procedural improvements), it is important to understand the upcoming changes.

Data Act and Data Governance Act

In January 2024, the EU Data Act (EU 2023/2854) entered into force. It aims to create harmonised rules on the fair access to and use of data. Together with the Data Governance Act (EU 2022/868), it forms an important part of the European strategy for data. The Data Governance Act entered into force in June 2022 and has been applicable since September 2023. It focuses on regulating processes and structures that facilitate voluntary data sharing. The Data Act complements the Data Governance Act. It regulates who can create value from data and under what conditions.

The Data Act is especially important because the Internet of Things (IoT) is becoming more common. The regulation ensures that connected products are designed and made so users can easily and safely access, use and share generated data. In general, raw and pre-processed data that are readily available to a data holder fall under the data-sharing obligations of the Data Act. The Data Act does not cover the protection of personal data. The GDPR applies to the processing of personal data under the Data Act.

You should comply when the connected product is placed on the EU market, or when the service related to the connected product is offered. The Data Act thus applies to data holders that are established inside and outside the EU. A 'data holder' is the entity that controls access to the data. The data holder can be a manufacturer of a connected product and/or a provider of a related service. Most parts of the Data Act will become applicable in September 2025.

Tips:

- Study the Data Act. Also read the Data Act explained and the FAQ on the Data Act.

See Article 50 of the Data Act for more details on its application.

See the European Data Governance Act, the Data Governance Act explained and the New practical guide to the Data Governance Act.

Set up clear procedures for data management within your company and make sure to monitor compliance with EU rules. You should also appoint people in the organisation who are responsible for keeping it up to date.

ePrivacy Directive

The ePrivacy Directive (2002/58/EC), commonly known as the 'cookie law', contains rules about the processing of personal data and privacy protection in electronic communications. It covers a wide range of topics, such as:

- Unsolicited commercial electronic messages ('spam');
- Restrictions on the use of cookies;
- The security of networks and services; and
- The processing of traffic and location data.

In 2017, the European Commission proposed a replacement for the ePrivacy Directive: the ePrivacy Regulation. The purpose was to provide more robust privacy protections in the digital age. However, in February 2025, the European Commission withdrew the proposal due to a lack of consensus and recognition that the proposal had become outdated. The withdrawal means that the ePrivacy Directive will remain in force, as will national laws (e.g. Law 34/2002 and Organic Law 3/2018 in Spain and Cookiebekendtgørelsen in Denmark).

Tips:

Read more about digital privacy on the website of the European Commission. It also publishes updates about reforms to European ePrivacy rules.

Keep records of consent forms.

Note that the legislation on data protection is only relevant if your services involve personal data. Make sure your staff is aware of your policy, so they do not unintentionally violate the GDPR.

General Product Safety Regulation

The General Product Safety Regulation (GPSR – EU 2023/988) came into force on 13 December 2024. Its purpose is to make sure that products on the EU market are safe for consumers. The GPSR replaced the General Product Safety Directive. The new regulation includes more future-proof product safety rules, such as rules for online sales, direct imports and technological products. It also includes cybersecurity measures and AI features to protect products from external threats and help them grow and learn.

The GPSR applies to physical and non-material consumer products, including software products and apps. It also applies to used, repaired and reconditioned products that are placed on the EU market. For example, you should make sure that your product is safe throughout its entire lifespan, including software updates. The GPSR does not include services, but it does include products provided to consumers as part of a service.

If you sell your product in Europe, you need a responsible person in the EU market who can act as a point of

contact for consumers and market surveillance authorities. If you provide services for a client, the client is responsible. However, you should still be aware of the safety rules.

Tips:

Make sure you understand the GPSR and know what your responsibilities and obligations are. Read the key changes introduced by the GPSR, a brief overview of the product safety legislation (including GPSR-related documents such as a factsheet) and a summary of the GPSR.

Prepare for the GPSR by performing a risk assessment to identify potential safety issues throughout the entire lifespan of your products. Also make sure to train your staff on the GPSR (including updates) so they can apply the regulation properly.

Product Liability Directive

In December 2024, the new Product Liability Directive (PLD – EU 2024/2853) entered into force. This Directive makes sure that consumers can claim compensation from manufacturers if a product causes them damage. This damage can include physical or psychological harm, damage to property, or the destruction or corruption of data.

The PLD will apply to products placed on the EU market as of 9 December 2026. The new Directive also includes rules for new technologies. All types of software are covered, including applications, operating systems and artificial intelligence (AI) systems. This means manufacturers of both products and components are responsible for any problems that occur once their software or AI system has been released on the EU market. It also covers defects caused by updates, upgrades or machine learning features.

If the manufacturer of a product or component is located outside the EU, the EU importer or authorised representative is responsible for the damage. However, be aware that the manufacturer is liable if anything happens.

Tip:

For a clear overview of the PLD, visit the EU's page on liability for defective products.

Artificial Intelligence Liability Directive

In 2022, the European Commission proposed an Artificial Intelligence Liability Directive (AILD) to complement the EU liability framework with specific rules for damages caused by AI. However, the proposal was withdrawn in February 2025 due to a lack of agreement. Nevertheless, you should stay up to date on developments.
The Commission work programme 2025 (Annexes) mentions that the Commission will evaluate if an alternative proposal should be presented or if they should choose another approach.

Artificial Intelligence Act

The Artificial Intelligence Act (AI Act – EU 2024/1689) sets uniform rules on AI. It is the first legal framework for AI in the world. Its purpose is to promote trustworthy AI in the EU. The AI Act gives clear guidelines for AI

developers and deployers on specific uses of AI. With these rules, the EU aims to ensure safety and fundamental rights, and support human-centric AI. The European AI Office and the national authorities implement, supervise and enforce the AI Act.

The rules apply to public and private actors. If you place an AI system on the EU market or if the use of the AI system affects people located in the EU, you must comply with the AI Act, even if you are located outside the EU.

The AI Act came into effect on 1 August 2024, but its application will happen in stages. Most of the requirements will be effective as of 2 August 2026. A few requirements will enter into application at a different point in time.

Timeline:

- 2 February 2025 – Prohibitions and AI literacy obligations entered into application.
- 2 August 2025 – The governance rules and the obligations for general-purpose AI models will enter into application.
- 2 August 2026 – The AI Act will become fully applicable (except for the rules for high-risk AI systems).
- 2 August 2027 – The rules for high-risk AI systems will enter into application.

The AI Act outlines four levels of risk for AI systems:

- Unacceptable risk: AI systems that are a threat to the safety or rights of people are banned. The AI Act prohibits eight practices, including harmful AI-based manipulation and deception, and biometric categorisation to identify or judge protected characteristics of an individual based on available information.
- High risk: AI use-cases that are a serious risk to health, safety or fundamental rights. For example, AI safety components in critical infrastructure and AI use-cases for providing access to important private and public services. They must follow strict rules to be allowed onto the EU market, such as risk assessments, high-quality datasets and proper human oversight measures.
- Limited or transparency risk: There are risks when people are not told about AI use. The AI Act requires companies to clearly state when AI is used, so people can make informed choices, like knowing when they are talking to a chatbot. Generative AI providers must also ensure that content created by AI is easy to recognise.
- Minimal risk: These AI systems are very safe and cause (almost) no harm. There are no rules for this category.

Figure 2: Risk levels for AI systems in the AI Act

Source: Globally Cool

To help companies prepare for the implementation of the AI Act, the European Commission (EC) started the AI Pact. The AI Pact consists of two pillars:

- In the first pillar, the AI Office will help stakeholders understand the AI Act. They will also explain how companies can prepare themselves for implementation. In turn, the AI Office learns about best practices and problems the participants face.
- The second pillar offers a framework to support the early implementation of certain measures of the AI Act.

Tips:

Follow the Implementation timeline of the Future of Life Institute (FLI) to stay up to date on the

implementation of the AI Act.

Study the AI Act. Does it apply to your company? If so, what do you need to comply with and when? You can use the following sources to get more insights: FLI's AI Act Explorer, Small businesses' guideline to the AI Act, EU AI Act compliance checker and the EC's AI Act Q&A.

Stay up to date on the AI Pact events organised by the AI Office. Join webinars and workshops to learn more about the AI Act and how it should be implemented.

Cyber Resilience Act

The EU's Cyber Resilience Act (CRA – EU 2024/2847) aims to improve cybersecurity for products (hardware and software) with digital elements. The Act addresses insufficient cybersecurity and the lack of timely security updates for these products. It sets cybersecurity requirements for their design, development and production. The Act also outlines the responsibilities of producers, importers and distributors to make sure cybersecurity is maintained throughout the product's lifecycle.

The CRA applies to companies that produce or sell products on the EU market that are connected to other devices or networks. This includes a wide range of products, such as IoT devices (e.g. smartwatches and webcams) and software that contains a digital component. However, it excludes items that are already covered by other regulations, like medical devices and cars. Non-commercial open source software is also excluded.

The CRA came into force on 10 December 2024, but there will be a transition period to give companies time to adjust. The rules laid down in the Act will apply as of 11 December 2027 with a few exceptions. The timeline below shows when each part will start to apply.

Timeline:

- 11 June 2026 – The provisions of the notification of conformity assessment bodies will apply (Chapter IV, Articles 35 to 51 of the CRA).
- 11 September 2026 – Reporting obligations of manufacturers will apply (Article 14 of the CRA).
- 11 December 2027 – The whole CRA regulation will apply.

Products covered by the CRA must have CE marking to show that they meet these requirements before being sold in the EU market.

Tip:

Make sure you understand the CRA regulation and the implications it has for your business. Visit the EU portal to learn more about the CRA regulation. Also check out the CRA Factsheet for a quick overview and the CRA Q&A for more detailed information.

Cybersecurity Act

The Cybersecurity Act is designed to strengthen cybersecurity and resilience within the EU. It has two primary objectives:

- Enhancing the European Union Agency for Cybersecurity (ENISA) by laying down its objectives, tasks and

organisational matters; and
- Establishing a framework for voluntary European cybersecurity certification schemes for ICT products, services and processes. The EU Cybersecurity certification framework will offer EU-wide schemes. These schemes include a full set of rules, technical requirements, standards and procedures.

In January 2024, the European Commission adopted Implementing Regulation (EU) 2024/482. This regulation sets rules for the adoption of the EU Cybersecurity Certification Scheme on Common Criteria (EUCC) – the first scheme adopted under the Cybersecurity Act. It is based on the international Common Criteria standard (ISO/IEC 15408). The EUCC scheme is voluntary and covers the certification of cybersecurity of ICT products (e.g. smartcards, specialised software and databases) in their lifecycle. The regulation includes rules for:

- The evaluation, issuance, renewal and withdrawal of EUCC certificates;
- Accredited conformity assessment bodies to issue certificates;
- Monitoring compliance and handling non-compliance; and
- Recognition agreements with non-EU countries.

The Implementing Regulation is applicable as of 27 February 2025. As such, the EUCC scheme has been available for vendors since 27 February 2025.

An amendment to the Cybersecurity Act was adopted on 15 January 2025. The amendment aims to enable the adoption of European cybersecurity certification schemes for managed security services. The EC had a public consultation to receive input to evaluate and revise the Cybersecurity Act until 20 June 2025.

Also make sure to stay up to date on any new cybersecurity certification scheme. For example, ENISA is working on the cybersecurity certification schemes, EUCS on cloud services and EU5G on 5G security.

Tips:

Read the summary of the Cybersecurity Act and the summary of the Implementation Regulation to familiarise yourself with the most important aspects of these legislations.

Visit the ENISA EU Cybersecurity Certification website for more information on the EUCC Certification Scheme, news & events, new and upcoming EU cybersecurity regulations and the development of certification schemes.

While it is not required yet, getting certified under the EUCC scheme can help build trust with EU clients, show your commitment to cybersecurity and give your company a competitive advantage in the European market.

NIS2 Directive

The NIS2 Directive sets measures for a high level of cybersecurity in the EU. With this directive, the EU wants to protect network and information systems (NIS), users and affected individuals from cyber threats. It applies to 18 critical sectors, which are divided into sectors of high criticality (see Annex I) and other critical sectors (see Annex II). Critical sectors include:

- Digital infrastructure, such as cloud computing service providers, data centre service providers and content delivery network providers (high critical sector);
- ICT service management (business-to-business), such as managed service providers and managed security service providers (high critical sector); and
- Digital providers, such as providers of online marketplaces, search engines and social networking platforms

(other critical sector).

For the critical entities, the directive lays down cybersecurity risk-management measures, reporting obligations and rules on cybersecurity information sharing. The NIS2 Directive has applied since 18 October 2024.

Tips:

For more information on the NIS2 Directive, see the European Commission's page on the NIS2 Directive and the frequently asked questions.

See Article 2 of the NIS2 Directive for details on the entities it applies to.

Digital Services Act

The Digital Services Act (DSA – EU 2022/2065) seeks to make the online environment safer for people and businesses in the EU. It contains rules to protect users and their rights. The DSA explains the responsibilities of online platforms and social media. It also sets out rules related to illegal content, illegal products, hate speech and false information. With this regulation, the EU aims to improve transparency through better reporting. It also supports new ideas, business growth and competition in the EU. The regulation has applied since 17 February 2024.

The DSA gives clear responsibilities and a system of accountability and transparency for providers of intermediary services. It applies to all providers (inside *and* outside the EU) that offer intermediary services to people or businesses located within the EU. This includes hosting services, app stores, social networks and domain name registrars. The regulation also has special rules for very large online platforms (VLOPs) and very large online search engines (VLOSEs).

Tip:

Read more about the Digital Services Act.

European Accessibility Act

The European Accessibility Act (EAA – EU 2019/882) is a directive on the accessibility requirements for products and services. There is high demand for accessible products and services for people with disabilities. As the number of people with disabilities is expected to grow, an environment with more accessible products and services helps to create a more inclusive society and helps them to live independently.

The Act focuses on products and services that are most important to people with disabilities:

- Consumer general-purpose computer hardware systems and operating systems;
- Self-service terminals like ATMs, ticketing and check-in machines;
- Smartphones;
- TV equipment related to digital television services;
- Telephony services and related equipment;
- Access to audio-visual media services such as television broadcast and related consumer equipment;

- Services related to air, bus, rail and waterborne passenger transport;
- Consumer banking services;
- E-books and dedicated software; and
- E-commerce services.

The directive is applicable as of 28 June 2025. This means products and services that will be placed on the EU market after 28 June 2025 have to comply with this regulation. For products and services placed on the EU market before that date, transitional measures apply. The directive only applies to companies in the business-to-consumers (B2C) segment; it does not apply to business-to-business (B2B). However, if your clients are in the B2C market, then you do have to comply.

Tips:

For more information on the EAA, visit the European Commission's page about the European Accessibility Act.

See Annex I of the EAA to get informed about the accessibility requirements for products and services.

See Article 32 of the EAA for more details on transitional measures.

Corporate Sustainability Due Diligence Directive

The European Green Deal is a roadmap for Europe to become a climate-neutral continent by 2050. As part of the Green Deal, the Corporate Sustainability Due Diligence Directive (CSDDD – EU 2024/1760) entered into force in July 2024. This irective requires companies to act in a sustainable and responsible way in their business practices and global supply chains. It sets rules for companies to identify and address problems that may harm human rights or the environment in their operations and subsidiaries, and amongst their business partners.

The directive applies to:

- Large EU companies: More than 1,000 employees with a net turnover of €450 million worldwide; and
- Large non-EU companies: A net turnover of €450 million in the EU.

Although small and medium-sized enterprises (SMEs) are not covered, the CSDDD may affect you through your buyers indirectly. As such, you should be familiar with the CSDDD requirements and what kind of information your buyers may need from you. This makes it easier for European companies to work with you and comply with the directive.

In February 2025, the European Commission adopted a package of proposals – the Omnibus package – to simplify sustainability due diligence rules. As part of this, the European Parliament agreed to postpone the application dates of the CSDDD. The Member States have to adopt and publish the directive into national law by 26 July 2027. On 26 July 2028, the directive will start to apply to the first group of companies. The CSDDD will be fully applicable as of 26 July 2030. Proposals to change the content and scope are not yet final, so make sure to stay up to date.

Tips:

If you do business with a large company, familiarise yourself with the CSDDD. This builds trust among business partners and shows professionalism.

Stay up to date on the developments of the Omnibus package.

Forced Labour Regulation

In December 2024, the Forced Labour Regulation (FLR – EU 2024/3015) entered into force. It bans products made with forced labour from the EU market. The EU follows the definition of forced labour of Article 2 of ILO Convention No. 29. The regulation applies to all products, including their components, regardless of their country of origin. The regulation will apply as of 14 December 2027. The European Commission will set up measures to support economic operators and their business partners, especially SMEs.

Tip:

Start early by checking your company for any risks of forced labour. Put simple due diligence measures in place to make sure you comply with the regulation in time and build trust with EU clients.

Ecodesign for Sustainable Products Regulation

In July 2024, the Ecodesign for Sustainable Products Regulation (ESPR – EU 2024/1781) entered into force. This Green Deal regulation aims to improve the sustainability of products that are placed on the EU market. It intends to improve products' circularity, energy performance, recyclability and durability. The ESPR applies to almost all physical products placed on the EU market, regardless of where they are produced. If you provide services for a client, the client is responsible for product sustainability. However, you should still be aware of the rules.

The process starts with the development of working plans. These plans will list the products that will need to meet ecodesign requirements and other measures that will be assessed. The first ESPR working plan will be published in the first half of 2025 and will cover at least three years. Among the products prioritised in the first working plan are energy-related products, ICT products and other electronics. The development of product rules will start once the first working plan is published.

The ESPR will replace the Ecodesign Directive (2009/125/EC). There will be a transition period in place until 2030 to make sure there is no gap.

Tip:

Make sure you understand and follow the developments of the ESPR. You can also watch the online information session on the ESPR. Assess what its impact will be for your company.

2. What additional requirements and certifications do buyers ask for in BPO or IT outsourcing?

European buyers often have additional requirements when choosing a BPO or IT outsourcing provider. These

mainly relate to quality, privacy, security and corporate social responsibility (CSR).

Information security

Information security relates to both data protection and data recovery systems. Many European buyers expect you to have an information security management system (ISMS), especially in industries in which security is essential, such as finance and banking, healthcare and mobile applications.

The ISO 27000 series contains common information security standards and guidelines. ISO 27001 is an internationally recognised standard with ISMS requirements. ISO 27002 supports ISO 27001. It provides guidance and advice on how to implement information security controls. Other supporting documents are ISO 27003 and ISO 27004.

Figure 3: What is ISO/IEC 27001?

Source: ISO @ YouTube

You should have a proper information security and management system in place that covers the necessary areas outlined in this standard, even if your buyer does not require formal certification.

ISO/IEC 27701:2019 certification is a certifiable privacy extension of ISO 27001 supporting GDPR. It specifies the requirements for implementing and maintaining a Privacy Information Management System (PIMS). To get certified to ISO 27701, you will either need to have an existing ISO 27001 certification or implement ISO 27001 and ISO 27701 together as a single implementation audit. The new ISO/IEC 27701 is under development and is expected to replace ISO/IEC 27701:2019 soon.

Tips:

> Make sure you have effective security processes and systems in place covering everything from business continuity and disaster recovery to virus protection.

Ask your buyers if they require ISO 27001 certification.

For the UK, check out the Cyber Essentials Scheme. This standard is especially relevant to organisations that process and control PII (Personally Identifiable Information).

Quality management

Some European buyers will only do business with companies that have a quality management system in place. Although having a system like this does not guarantee high-quality IT solutions or business process services, it does show that you have a repeatable process and you are a serious company that values standardisation. ISO 9001 and the Capability Maturity Model Integration (CMMI) are the most widely used quality management systems in outsourcing. Even if you have a good in-house quality management system, buyers prefer systems they recognise.

ISO 9001:2015

One of the best-known quality management standards is ISO 9001:2015. You can obtain certification, but this is not a requirement.

ISO 9001:2015 certification or compliance means the organisation (or part of it) has demonstrated that:

- It follows the guidelines of the ISO 9001 standard;
- It fulfils its own requirements;
- It consistently meets customer requirements and statutory and regulatory requirements; and
- It keeps records.

Figure 4: What is ISO 9001?

Source: ISO @ YouTube

ISO/IEC/IEEE 90003:2018 guides you in applying ISO 9001:2015. It specifically focuses on computer software and related support services.

ISO is working on a new standard, ISO/CD 9001.2, to replace ISO 9001:2015. The committee is currently reviewing the draft.

Capability Maturity Model Integration (CMMI)

Another option for quality management is the CMMI, which has been adopted worldwide. You can achieve a maturity level rating from 1 to 5. It indicates your capability in multiple process areas, including product development, service excellence, workforce management, supplier management and cybersecurity. CMMI Services then helps you improve your capability to provide customers with quality services.

> Tip:
>
> Consider working towards ISO 9001:2015 compliance, even if you do not plan to get full certification right away. This shows European buyers that your company follows a structured quality process, keeps records, and is serious about meeting customer expectations.

ISO standards for software development

ISO standards help companies create good quality software. They give clear rules and guidelines for every part of software development. Again, complying with such standards shows you run a professional company with repeatable, transparent processes.

Important ISO standards for software development include:

- ISO/IEC/IEEE 12207:2017: This standard explains processes for defining, controlling and improving the lifecycle of software processes. The standard will be replaced by ISO/IEC/IEEE DIS 12207.
- ISO/IEC/IEEE 15288:2023: This standard describes the system lifecycle processes. It defines processes to facilitate system development and information exchange.
- ISO/IEC/IEEE 29119-1:2022: This standard presents general concepts in software testing and key concepts for the ISO 29119 series.
- ISO/IEC 33000 series: This series is about software process assessment. It gives a framework for the assessment of process capability and organisational maturity.
- ISO/IEC 25000 series: This series deals with Systems and software Quality Requirements and Evaluation (SQuaRE).

These standards do not offer the option of certification.

> Tip:
>
> Study these standards and apply the most appropriate of them to optimise your software development services.

Agile project management

European buyers may expect you to work in an Agile way. This approach is based on the Agile Manifesto. An Agile method is a flexible approach to managing projects that allows you to adapt to changes. Instead of delivering one final product, it divides projects into smaller iterations (sprints). Collaboration amongst team members and other stakeholders is at the core of this method. People work together in self-organising and cross-functional teams.

Figure 5: Agile methodology

Source: CBI

Examples of popular Agile methods are:

- Scrum: A framework that divides work into time-boxed sprints. It has defined roles, like scrum masters and product owners, to guide the team. It focuses on regular meetings (sprints) to review progress and adapt quickly;
- Kanban: A visual approach to managing work. It uses boards to track tasks and maintain an overview of the workflow process. It supports continuous delivery and emphasises steady workflow improvements;
- Extreme Programming (XP): A framework that emphasises technical excellence through practices like pair programming, test-first programming and frequent small releases. It is based on communication, simplicity, feedback, courage and respect. It aims to improve software quality and the quality of life of the development team;
- Feature-Driven Development (FDD): A model-driven process that focuses on designing and building features in short iterations. It breaks down the project into client-valued functions for efficient progress tracking. It is a good approach for large-scale, long, and complex projects; and
- Scaled Agile Framework (SAFe): A set of principles and practices for scaling agile across large enterprises and multiple teams. It aligns teams under a common framework. SAFe is used at three levels: the individual team level, the programme level and the portfolio level, which contains multiple programmes.

A range of certifications are available for people who work with Agile frameworks, such as:

- Certified Scrum Master (CSM);
- Professional Scrum Master (PSM);
- Certified Scrum Product Owner (CSPO);
- PMI-Agile Certified Practitioner (PMI-ACP);
- AgilePM Foundation;
- ICAgile Certified Professional;
- SAFE Product Owner/Product Manager (SAFe POPM); and
- Certified Agile Project Manager (IAPM).

Tips:

Make sure to check with European buyers which Agile method they use (if any) and what they expect from you.

Check out the Agile Glossary of the Agile Alliance and the Glossary of ProductPlan to learn more about the different Agile methods.

For insights into the different certifications for Agile project management, see ScrumAlliance's overview of Agile Certifications.

Sustainability and ESG

Companies are increasingly required to demonstrate their sustainable business practices. ESG stands for environmental, social and governance. It is used to measure the sustainability and ethical impact of companies. ESG is often mentioned alongside sustainability and Corporate Social Responsibility (CSR). All the concepts are related and important. While CSR and sustainability cover the broader ideas and goals of social and environmental sustainability, ESG is more concrete and offers a measurable approach.

ESG is important for companies that operate in the BPO and IT outsourcing industry to attract investment, ensure legal compliance and meet growing demand from clients for more sustainable business practices. For example, the UK's largest association for contact centres, CCMA, says that ESG commitments are a prerequisite for buyers and clients in today's supply chain. BPO providers might lose business opportunities if they cannot prove their ESG commitments and deliverables.

Voluntary sustainability standards and initiatives

Voluntary sustainability standards can help you demonstrate social and environmental responsibility. For example:

- ISO 26000: Provides guidance on integrating social responsibility into business strategies;
- ISO 14001: Sets criteria for an environmental management system (EMS), which you can achieve certification for;
- B Corp Certification: Recognises businesses that meet strict standards of social and environmental performance, accountability and transparency.

Impact sourcing

You can make a social impact by becoming an impact sourcing provider. Impact sourcing aims to improve the lives of individuals, families and communities through meaningful employment in IT and business process outsourcing (ITO and BPO). This can be achieved either through outsourcing or by setting up remote or virtual teams using digital technology.

However, sourcing and training these people requires quite some upfront investment and effort from you as their employer. You can look for support from local impact sourcing initiatives, work readiness programmes, and (non-profit) training institutes.

When you have tackled this challenge and set up an effective recruitment and training strategy, you can enjoy the benefits:

- A large(r) talent pool in a competitive market;
- A loyal and motivated workforce;
- A strong competitive advantage; and
- A positive social impact on your employees and community.

For your buyers, this means:

- Better supplier performance;
- A stable/reliable supplier workforce;
- Meeting inclusion and diversity goals; and
- Making a positive social impact.

Fair-trade software

Another example of how sustainable initiatives extend to small IT businesses is fair-trade software. This is software that is developed for better prices, under decent working conditions, while supporting local sustainability and with fair terms of trade. In essence, fair-trade software is part of the broader concept of impact sourcing.

Tips:

- Implement sustainable business practices and clearly communicate these in your marketing activities. Also, show that you care about your impact on society and the environment by implementing your own CSR policy. This can be a unique selling point (USP) for buyers when selecting a provider.
- Use a self-assessment, like FormIGA's Service Provider Sustainability Index (SPSI), to assess your sustainability and ESG maturity. This tool was specifically created for service providers in the technology and business services sector.
- For more information on sustainability and CSR, see our studies Tips on how to go green and Tips on how to become more socially responsible.
- Consult the ITC Standards Map for a full overview of certification schemes that address sustainability in the outsourcing sector.
- If you are an impact sourcing provider or a fair-trade ITO or BPO provider, use this in your unique value proposition (UVP) to promote yourself. First, make sure to check if you meet the requirements for impact sourcing suppliers. For more information about fair-trade software, see the Fair Trade Software Foundation and Web Essentials' video on what fair trade software development means.

Table 1: Most important certifications requested by buyers in the BPO and IT outsourcing sector

Name	Type	Cost	Most used in European end-market(s)	Further information
ISO 27001	Information security	Varies depending on factors like company size, the complexity of your ISMS and the certification body.	All	You can apply for certification via an accredited certification body.

ISO 9001	Quality management	Varies depending on factors like company size and complexity and the certification body.	All	You can apply for certification through an accredited certification body.
CMMI	Quality management	Varies depending on factors like company size, location, context and appraisal type and scope. You can get an idea of cost via a CMMI Partner.	All	CMMI certification is available for individuals, not companies. Your company can be CMMI-appraised, not certified.
Agile methodologies	Project management	Varies depending on the specific certification.	All	Agile certification is available for individuals but not companies.
GDPR compliance	Data protection	Varies depending on factors like company size, complexity and compliance type.	All	Companies can demonstrate compliance with GDPR through third party audits or statements of compliance. Check out the scheme owners of the EU Data Protection Seal and national certification criteria.

Source: Globally Cool

3. What are the requirements and requested certifications in the niche outsourcing markets?

European buyers often require compliance with sector-specific and/or service-specific standards or codes of practice. Examples of sector-specific standards are the Basel Committee standards for banking. Service-specific standards include those for cloud service providers and payment-related services.

Financial services

The European Banking Authority's (EBA) Guidelines on outsourcing arrangements took effect on 30 September 2019. These guidelines apply not only to banks, building societies and investment firms, but also to payment institutions and electronic money institutions.

The PCI Security Standards Council (PCI DSS) is a global forum for the payment industry. It maintains, develops, and promotes Payment Card Industry Security Standards. If you work with payment-related services and want to offer outsourcing services to the European market, see their standards overview and do the Self-Assessment. This will help you get insights into the standards for payment-related services.

IoT-related services

ETSI EN 303 645 and ETSI TS 103 645 are important standards for cybersecurity for consumer IoT. ETSI is a European Standards Organisation (ESO) and the recognised regional standards body for telecommunications, broadcasting and other electronic communications networks and services in the EU. It released the first globally applicable standard for consumer IoT security. Other organisations have also developed security guidelines for IoT, which can be found on the websites of Entrust, GSMA and SENKI.

Cloud service providers

CISPE.cloud has developed a sector-specific code for cloud infrastructure service providers under Article 40 of the GDPR. They have a page dedicated to helping organisations accelerate the development of GDPR-compliant cloud-based services for consumers, businesses and institutions.

Other niche markets

Specific buyer requirements also apply in other major European industries, such as aviation, automotive and agriculture. Some requirements are software and/or technology related. Standards, frameworks and guidelines are available for many different industries. Examples of sector and service-specific buyer requirements are ISO 18295-1:2017 for contact centres, and HL7 and HIPAA for health and social care. Check which standards, guidelines and industry bodies are important for your specific country and industry.

Tips:

- Learn which standards are relevant to the services you provide. Buyers will expect this from you. Do your research in advance, so you can show that your company complies with these standards.
- Check which sector-specific standards or codes are available for your specific product, for example by asking your sector association or buyer. Also ask buyers to what extent they want you to implement these standards.
- Look at the product and services-specific buyer requirements for big data, blockchain, contact centre services, cyber security, finance and accounting, retail tech, software development services, software testing services, virtual reality and augmented reality and others on our market information page.
- Some standards have competing equivalents, especially in smaller and more specific industries. Keep

track of which standards exist for your product/market combination to ensure you comply with the most relevant ones.

Globally Cool carried out this study in partnership with Laszlo Klucs on behalf of CBI.

Please review our market information disclaimer.