What requirements must outsourcing services comply with for the European market?

Last updated:
07 February 2022

Requirements and standards continue to be very important in the outsourcing industry. Main mandatory requirements concern copyright and data protection. Important common requirements are the presence of a quality management system, corporate social responsibility, but also a relatively new term: “digital resonance”.

New requirements emerge annually, you have to continuously monitor what standards and guidelines are important for your product-market combination.

Contents of this page

1. What are mandatory requirements?

Mandatory outsourcing requirements for the European market can be divided into legal and non-legal mandatory requirements. Although non-legal requirements are not obligatory by law, they are considered minimum requirements to enter the European market.

Legal mandatory requirements

Legal mandatory requirements are requirements that are both legal and mandatory for companies entering the European outsourcing market. Legal requirements include legislation about copyright, personal data protection, the general data protection regulation and the e-Privacy Directive.

We advise you to check the exact rules in your European target market. On the ePing website (an initiative by WTO, ITC and the UN), you can find an overview of country-specific measures that affect trade and that are not the same as the international standards. On the ePing website you can also find the contact persons per country that the World Trade Organisation (WTO) has appointed. You can subscribe to receive ‘e-Ping alerts’ that might be relevant for your product or service.

Copyright

Copyright refers to legal protection of computer programs. The European Union has established specific rules to protect computer programs by means of copyright. According to the directive on the legal protection of computer programs you have to make sure not to breach any copyright when placing your computer program on the market and at the same time your products are also protected against unauthorised reproduction under this directive (law).

Tips:

Read more on the legal protection of computer programs on the website of the European Commission.

Check the exact regulations in your European target market. All European Union member states have implemented the European Directive into national legislation. Although they are generally the same, there could be minor differences.

Pay attention to copyright and infringement (the act of breaking or disobeying the contract) clauses in the contracts you sign with European buyers.

Personal data protection

Privacy is highly protected in Europe. The European Union has several directives in place for this purpose. Providers that do not respect these directives may be subject to enforcement actions and/or possible claims - even if they are located outside Europe.

General data protection regulation

The General Data Protection Regulation (GDPR) is designed to protect individuals in Europe from privacy and data breaches. It aims to give people more control over their personal data and let businesses benefit from a level playing field. The GDPR applies to all companies processing the personal data of individuals in Europe, regardless of the company's location. This means it also applies to you directly.

Under the GDPR, any company or individual that processes data is responsible for its protection. Examples of protected personal data are names, email addresses, bank details, social media content, photos and IP addresses.

Some key consumer rights you must comply under the GDPR with include, but are not limited to:

- consent – consumers must explicitly consent by opting in, consent must be easy to withdraw, and requests must be specific and in plain language
- right to access – consumers are entitled to know whether companies process their personal data, where they do so, and for what purpose
- right to be forgotten – consumers are entitled to have their personal data erased, and to have processing and further dissemination halted
- privacy by design – data protection should be included from the onset of designing systems; data collection should be minimised, and access limited

Tips:

If you deal with personal data, study the GDPR's European data protection rules and principles for a good understanding of what is allowed and what is not. For the situation in the UK after Brexit, check out the website of the UK Information Commissioner's Office.

Audit your current data to determine whether it is GDPR compliant. What data do you have, where and why? Did you or your client obtain explicit consent to use it for this specific purpose?

Set up clear consent request forms and privacy policies that inform your and your client's customers how you process their personal data. For more information, see GDPR: How to create best practice privacy notices (with examples).

Use IDC's GDPR Readiness Assessment to determine how compliant you are and what you may need to improve.

ePrivacy Directive

The ePrivacy Directive, commonly known as the “cookie law”, contains specific regulations for data protection in the electric communications sector. Examples of actions that are now controlled by the e-Privacy Directive are; sending unsolicited commercial electronic messages (‘spam’). This is no longer allowed. There are strict rules on the use of cookies and contact details may only be published with consent of the subject.

A new ePrivacy Regulation was originally scheduled to enter into force along with the GDPR, but its implementation has since been delayed. The latest proposal was released in February 2021, with a mandate for negotiations with the European Parliament. The new regulation is intended to safeguard the confidentiality of electronic communications through stronger privacy rules. Unlike the current directive, it includes internet-based voice and messaging technologies such as Skype, WhatsApp and Facebook Messenger.

Tips:

Keep records of your obtained consent.

Be aware of what data you store and where, to be able to comply with potential consumer requests. Also 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 GDPR regulations.

Read more on digital privacy on the website of the European Commission. This is also where you can keep up to date on the reforms of the European ePrivacy rules.

Contact Open Trade Gate Sweden if you have specific questions regarding rules and requirements in Sweden and the European Union.

Non-legal mandatory requirements

There are also non-legal requirements that are regarded mandatory by many European buyers of outsourcing services. Although these non-legal requirements are not obligatory by law they are minimum requirements to enter the European market. Without fulfilling these requirements your services will be unlikely to be considered by European buyers.

Information security

Information security is one of the main challenges for IT outsourcing service providers. This includes both data protection and recovery systems. Many European buyers expect you to implement an information security and management system, especially in industries in which security is essential, such as finance and banking, healthcare or mobile applications. The ISO 27000-series contains common standards and guidelines for information security.

ISO 27001 is an internationally recognised standard that provides requirements for an information security management system. The ISO 27002 standard can be a supporting document to ISO 27001. It gives guidance and advice on the implementation of information security controls. A company cannot be ISO 27002 certified, because it is only a guidance document. The company can be ISO 27001 certified. Other supporting guideline

documents in the ISO 27000-family are ISO 27003 and ISO 27004.

Tips:

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

Ask your buyer to what extent they require you to implement a security management system like the ISO 27001 standard.

Take into consideration obtaining the ISO/IEC 27701:2019 certification. This is a certifiable privacy extension of ISO 27001 supporting GDPR. Organisations looking to get certified to ISO 27701 will either need to have an existing ISO 27001 certification or implement ISO 27001 and ISO 27701 together as a single implementation audit.

2. What additional requirements do buyers often have?

European buyers often have additional requirements that are important to them when choosing an outsourcing provider. These refer to quality, privacy, security, and corporate social responsibility.

Quality management

Some European buyers only do business with companies that have a quality management system in place. Although it does not guarantee high-quality IT solutions or business process services, it proves that you have a repeatable process and that you are a serious company that values standardisation. Acknowledged and common quality management systems are ISO 9001:2015 and the Capability Maturity Model Integration.

ISO 9001:2015

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

Achieving ISO 9001:2015 certification, or complying with it, means that an organisation (or part of it) has demonstrated the following:

- It follows the guidelines of the ISO 9001 standard
- It fulfils its own requirements
- It meets consistently customer requirements and statutory and regulatory requirements
- It maintains documentation

ISO/IEC/IEEE 90003:2018 is a guideline (checklist) on how to apply ISO 9001:2005 for software development.

Capability Maturity Model Integration

Another option is the Capability Maturity Model Integration (CMMI), which has been adopted worldwide. You can achieve a 1-5 maturity level rating, indicating your improvement in multiple process areas, including product development, service excellence, workforce management, supplier management and cybersecurity. CMMI Services helps you to improve your capability to provide your customers with quality services.

ISO 9001 and CMMI are the most commonly used quality management systems in the outsourcing market. Even if you have developed a good in-house quality management system, buyers prefer a system they recognise. However, you need to realise that having ISO 9001 or CMMI certification is not necessarily a strong selling point (ISO 27001 is a little more important in certain market segments). On the other hand, if you are a company that

focuses on specific industries, complying with important standards, guidelines and/or frameworks applicable to that industry, it can be an interesting selling point, and a proof of your competence in that particular industry.

Digital Resonance

Digital resonance is increasingly important to European buyers. This term is used to describe how companies in a particular country, and their government handles the effects of digital transformation, in particular automation and cybersecurity.

Digital resonance is defined by a combination of:

- digital skills of a country's workforce
- legal and cybersecurity
- corporate investment in start-ups
- digital innovation outputs

The digital resonance level of your company is so important because European companies are increasingly relying on outsourcing and automation. This makes the systems more vulnerable. Many companies outsource vital functions or share sensitive information with their service providers. Yet, they do not understand the process enough to understand the risks.

The global management consulting firm Kearney also recognises the importance of digital resonance. In their biannual Global Service Location Index (GSLI), they added Digital Resonance as one of the factors to measure the competitiveness of an outsourcing destination. The four factors are: how attractive your destination is financially, its people skills and availability, the business environment and digital resonance.

The index is used by companies to understand and compare potential outsourcing locations. You can use the index to see how well your destination is doing, compared to other destinations and compared to other years.

Tips:

Check your countries score on the GSLI and see where you might need to improve. Improve your digital resonance. Make sure your employees have the skills to manage automation and cybersecurity. Also invest in solid data security and privacy (see trend below).

Show that you are a professional company, by having good references, obtaining relevant industry certification, responding quickly, communicating regularly, offering constant quality, complying with contractual agreements, and having a good and stable management team to lead the outsourcing project.

While quality management systems do not guarantee automatically "good quality software", having one implemented and consistently used helps greatly to produce good quality software. Invest in implementing (and using) a quality management system in your company.

Corporate Social Responsibility

Corporate Social Responsibility (CSR) refers to companies taking responsibility for their impact on the world. Not only in the products or services they offer, but also when it comes to:

- consumer rights
- education and training of staff
- human rights
- health

- innovation
- the environment
- working conditions

Its importance for the IT outsourcing (ITO) industry is debated, as the impact from small companies in this business is often marginal.

Documented CSR policy

CSR is becoming particularly important to large companies and governments in Northern and Western Europe. Many European companies involve their suppliers in their CSR policies. Having a well-documented CSR policy may give you a competitive advantage over companies without one. The ISO 26000 standard provides guidance on CSR. For small software companies, the most relevant and practical aspects of this standard are labour practices, fair operating practices and community involvement.

Impact sourcing destination

You can also match the CSR policy of your potential buyer by becoming an impact sourcing destination. Impact sourcing is a relatively new term. It is a sourcing model that aims to improve people's lives, families, and communities through meaningful employment in ITO and BPO. This can be achieved either through outsourcing or by setting up remote or virtual teams using digital technology. Thus, by creating jobs for those most in need, Impact sourcing has good potential for companies that wish to make their business more socially responsible (both buyers and sellers). And it can be a Unique Selling Point (USP) for your business.

Fair trade software

Another example of how CSR initiatives extend to small IT businesses is fair-trade software. It means software that is developed for better prices, under decent working conditions, supporting local sustainability and with fair terms of trade. In essence, fair-trade software is a part of impact sourcing. Impact sourcing has a wider reach than fair trade software.

Tips:

Clearly communicate your commitment to CSR in your marketing activities. Also, show that you care about your impact on society and the environment by implementing your own CSR policy. It can be a unique selling point (USP) when your buyer has to select a provider.

Consider profiling yourself as an impact sourcing provider or a fair-trade ITO or BPO provider. See if you meet the requirements for impact sourcing supplier. For more information about fair-trade software, see the Fair Trade Software Foundation and Web Essentials' video on what fair-trade software development means.

Consult the ITC Standards Map for a full overview of certification schemes addressing sustainability in the outsourcing sector.

3. What are the requirements for niche markets?

European buyers often require you to comply with a sector-specific and/or industry specific standard, or code of practice (if available). Examples of industry specific standards are Financial Services, Basel Committee Standards. Examples of Service specific standards are Cloud service providers and Payment related services.

Financial services

From 30 September 2019, the European Banking Authority's (EBA) guidelines on Outsourcing Arrangement took effect. This law does not only apply to banks, building societies and investment firms, but also to payment institutions and electronic money institutions.

The Basel Accords is a set of recommendations for regulations in the banking industry. It is developed by the Basel Committee on Banking Supervision. Basel I is the minimum requirement, often not accepted by European clients. Aim to get the Basel II and/or Basel III standard.

(Industrial) Internet of Things related services

ETSI TS 103 645 is an important standard for consumer security in Internet of Things (IOT). They released the first globally applicable standard for consumer IoT security. There are also other organisations that have developed security guidelines for the IoT. It is important to keep an eye out for other standards that are being developed and might increase in importance in the upcoming years. Other organisations that have developed security guidelines for IoT can be found at the NCIPHER website, the website of GSMA and the SENKI website.

Cloud service providers

The Cloud Industry Forum has released a Code of Practise for Cloud Service Providers. They updated their Code in 2017 to incorporate key components of the General Data Protection Regulation. Cloud service providers aiming for the EU/EFTA market are recommended to follow this code of practice.

Payment related services

The PCI Security Standards Council is a global forum for the payment industry. It maintains, evolves and promotes the Payment Card Industry Security Standards. If you are working with payment related services and (aim to) offer outsourcing services to the EU/EFTA market, look at their standards overview and complete their Self Assessment tool to get more insight on the standards on payment related services.

Other niche markets

There are other important European industries to which specific buyer requirements apply, like aviation, automotive or agriculture. The requirements can be software and/or technology related. There are standards, frameworks and (quality) guidelines available for many different industries. Examples of such sector/service specific buyer requirements are ISO 18295-1:2017 for Contact centres and HL7 and HIPAA for Health and social care. Check what standards, guidelines and industry bodies are present in your relevant country and industry-specific situation.

Tips:

Know which standards are relevant for the services you provide as buyers expect you to. Do your research in advance, so you can show them 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 your buyer. Also ask your buyer to what extent they want you to implement these standards.

Some standards have competing equivalents. Especially the less common ones and the industry specific standards. Keep an eye on the competing guideline companies to make sure you comply with the most relevant standards for your product/market combination.

If you are working in the Contact Centre industry, consider obtaining COPC certification. They have solutions designed for Work-At-Home environments for contact centre employees, if this situation applies to you.

Visit the EU Trade Helpdesk for more information on import rules and taxes in the European Union.

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 at the market information page of the CBI website.

This study has been carried out on behalf of CBI by Globally Cool B.V. in collaboration with Laszlo Klucs.

Please review our market information disclaimer.

Follow us for the latest updates

(opens in a new tab) Twitter

(opens in a new tab) Facebook

(opens in a new tab) LinkedIn

RSS