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

Service providers wanting to enter the European outsourcing market have to comply with several requirements. The main mandatory requirements concern the protection of copyright and personal data. Important common requirements are the presence of a quality management system and corporate social responsibility. Niche market requirements are industry or service-specific. Requirements and standards continue to be very important in the outsourcing industry. New requirements emerge annually and continue to impact the industry.

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.

Copyright

Copyright refers to the 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. 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 this is 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 new General Data Protection Regulation (GDPR) came into effect on 25 may 2018. This regulation was designed to protect individuals in Europe from privacy and data breaches. Since then, it has also been incorporated into the European Economic Area (EEA) Agreement, so the new GDPR is also enforced in Iceland, Liechtenstein and Norway.

These new rules were introduced to give people more control over their personal data and let businesses benefit from a level playing field where the laws and regulations are the same in every country. 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 old directive, the protection of any data by which an individual can be identified was the sole responsibility of the data controller (owner). However, under the GDPR, any company or individual that processes data is also responsible for its protection. Examples of personal data protected by this regulation are names, email addresses, bank details, social media content, photos and IP addresses.

Some key consumer rights you must comply with include, but are not limited to, consent (also known as permission or approval), the right to access, the right to be forgotten and privacy by design.

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 or not 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 have processing and further dissemination halted.

Privacy by design – data protection should be included from the outset when designing systems. Data use should be minimised and access limited.

Tips:

- Make sure you comply with the GDPR if you process data of European citizens (or sensitive information of any kind).
- Study the GDPR’s new European data protection rules and principles if you are dealing with personal data. This will give you a good understanding of what is allowed and what is not.
- 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 of how you process their personal data. For more information, see the GDPR consent guidance from the United Kingdom’s Information Commissioner’s Office and Econsultancy’s 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.
- Check the Eping website for an overview of country-specific measures that affect trade and differ from the international standards as well as for the contact persons per country that the WTO has appointed. You can also subscribe to receive alerts (called epingalerts) that might be relevant for your

product or service.

ePrivacy Directive

The ePrivacy Directive (2002/58/EC), commonly known as the “cookie law”, contains specific regulations for data protection in the electric communications sector. An example of an action that is now controlled by the ePrivacy Directive is 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 draft dates from February 2019 and it is expected to enter into force at the end of 2019. The regulation is intended to safeguard the confidentiality of electronic communications through stronger privacy rules. Unlike the current directive, it includes internet-based voice and internet-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, so you can 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 are 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 changes to 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 as 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.

Security

Data 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 considered to 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.

Consider obtaining the ISO/IEC 27701:2019 certification. This is a certifiable privacy extension of ISO 27001 supporting the GDPR. Organisations looking to get ISO 27701 certified 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

Many European buyers only do business with companies that have a quality management system in place. Such a system shows that you are well organised and are able to deliver the required service quality. They include, for example, back-up and recovery schemes, network and infrastructure security, communication plans and relocation options. 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 consistently meets 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. CMMI Services helps you to improve your capability to provide your customers with quality services.

Tips:

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 automatically guarantee "good-quality software", implementing and consistently using such a system will help greatly in producing 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 concerning consumer rights, education and training of your staff, human rights, health, innovation, the environment and working conditions. For the IT and IT-related services outsourcing industry, its importance is debated, as the impact of small companies is often marginal.

CSR is becoming especially important to large companies and governments in Northern and Western Europe. Many European companies involve their suppliers in their CSR policies. In the future, CSR may well become a direct selection criterion. Having a well-documented CSR policy may therefore give you a competitive advantage over companies without one.

ISO 26000 provides guidance on CSR. For small IT and IT-enabled services outsourcing companies, labour practises, fair operating practises and community involvement are the most relevant aspects of the ISO 26000 standard.

There are some new trends and initiatives to extend CSR to small IT businesses. Fair trade software is an example of such an initiative. This is software that is developed for better prices, under decent working conditions, supporting local sustainability and with fair terms of trade.

Impact sourcing is another example. Impact sourcing is described as the integration of disadvantaged workers from low-employment areas into the processes of businesses from more economically advanced countries, either through outsourcing or by setting up remote or virtual teams using digital technology.

This makes impact sourcing a perfect fit for the IT and IT-enabled services outsourcing from developing countries. Impact sourcing has good potential for companies that wish to make their business more socially responsible.

Tips:

Read more about Corporate Social Responsibility in practice on the website of the European Commission.

Look at examples of small software companies engaging in CSR.

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.

Clearly communicate your commitment to CSR in your marketing activities.

Consult the ITC Sustainability Map for a full overview of certification schemes addressing sustainability in the IT 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 and the 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 applies not only to banks, building societies and investment firms, but also to payment institutions and electronic money institutions.

Basel Committee Standards

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

Other main European industries (in addition to financial services) to which sector-specific buyer requirements apply in relation to IT outsourcing are subject to sector-specific regulations that may include requirements related to outsourcing. Check the relevant country and industry-specific regulator for applicable regulation. Examples of sector/service-specific buyer requirements include COPC certification or ISO 18295-1:2017 for contact centres and HL7 and HIPAA for health and social care.

Internet of Things-related service providers

ETSI TS 103 645 is an important standard for consumer security in the Internet of Things. There are a number of organisations that have developed security guidelines for IoT. It is important to keep an eye out for other standards that are being developed and might increase in importance in the coming years. Other organisations that have developed security guidelines for IoT can be found on the NCIPHER website, the GSMA website and the SENKI website.

Cloud service providers

The Cloud Industry Forum has released a Code of Practice for Cloud Service Providers. The forum updated its 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 into the standards on payment-related services.

Tips:

Implement ISO 9001 or CMMI (maturity level 3-5). These 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. The maturity level (ranking from level 0 to level 6) describes how far along in the implementation process your company is.

Know which standards are relevant for the services you provide. Buyers will expect this from you. 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.

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

This study has been carried out on behalf of CBI by Globally Cool.

Please review our market information disclaimer.