

# Information security applications in Europe

Europe is the second largest market for information security after North America. As the threat to information security continues to grow, so does spending on security applications. Technological developments like cloud computing and the Internet of Things also drive the demand for information security. European companies increasingly recognise the importance of addressing information security issues. This makes Europe a promising market for you.

## Contents of this page

1. [Product description](#)
2. [What are the challenges when it comes to outsourcing information security application development?](#)
3. [Which European markets offer opportunities for information security application development?](#)
4. [What trends offer opportunities on the European market for information security applications?](#)
5. [What requirements should information security services comply with to be allowed on the European market?](#)
6. [What competition do you face on the European information security application market?](#)
7. [Through what channels can you get your information security application services on the European market?](#)
8. [What are the end market prices for information security applications?](#)

## 1. Product description

### What are information security applications?

Information security applications prevent, protect, detect and respond to security risks of computers, software or networks.

They provide for example:

- information backups
- failure recovery
- protection from hacking

There are many types of information security applications, including:

- antivirus
- back-up and recovery
- information encryption
- information erasing
- information masking
- firewall
- spyware removal

### Why do European companies outsource information security application development?

#### Cost reduction

[For 60% of executives, cost reduction is their main reason for outsourcing IT.](#) This confirms that cost reduction continues to be the main driver for European companies to outsource IT services like information security application development.

#### Tips:

Offer competitive pricing, but don't compromise on the quality of your services.

Be transparent in cost benefits: avoid hidden costs.

## Industry expertise and reputation

Another key advantage of outsourcing information security services is that European companies don't need to hire in-house expertise. When they select a service provider, relevant industry expertise and track record are important selection criteria. They look for specialists in a specific service or industry. To make sure their operational needs are met, European companies may require a try-before-you-buy experience. For example, a pilot project or online demo.

### Tips:

Specialise in a specific vertical, horizontal or niche market. Identify what your company does best and focus on doing that better than anyone else. This gives you added value and a unique selling proposition.

Emphasise your specific expertise in your marketing activities.

Use customer testimonials about the quality of your services, ease of transition and the benefits of your services. This proves your expertise and enhances your reputation.

Offer potential buyers a pilot project or demo to demonstrate your capabilities and gain trust.

## 2. What are the challenges when it comes to outsourcing information security application development?

### Data security

Data security is one of the main challenges in outsourcing. [Global information breaches can often be linked to outsourced IT services](#). This makes data security of the utmost importance to European companies considering outsourcing information security application services.

European companies generally perceive offshore data security to be of inferior quality. [The European Union currently considers data appropriately protected in a select number of countries](#):

- the 28 countries of the European Union
- the three countries inside the European Economic Area - Iceland, Liechtenstein and Norway
- countries with "adequate" data protection laws - Andorra, Argentina, the British Islands, Canada, Faroe Islands, Israel, New Zealand, Switzerland and Uruguay, as well as the United States of America (limited to the [Privacy Shield framework](#))

This makes it even more important for you to show potential European buyers that your services are secure.

### Tips:

Provide clear information about your company's data security and privacy measures.

Invest in a secure, reliable infrastructure.

Apply for security standards like the [ISO 27000-series on information security](#) to support your commitment to data security.

Make sure you comply with [European data protection rules](#). Look at the requirements section for more information.

## Integration capability

Information security applications need to be compatible with a company's existing infrastructure. This integration capability is an important requirement when selecting a service provider.

### Tips:

Offer information security applications that are easily integrated with other tools/solutions. Select for example technologies that are based on open standards. These are publically available standards whose specifications can generally be implemented on a royalty-free basis.

Provide support in the implementation and integration of your security applications.

## Clear communication

Good communication between customer and service provider is essential to providing information security application services. Unclear communication may cause misunderstandings and disagreements, which can lead to disputes with your buyer.

Providing good security application services begins with defining what the application should do. For example:

- What should the application secure?
- What are the infrastructure components in should be compatible with?

The extent of communication with your buyer a project requires depends on the type of contract:

### Fixed

With a fixed price contract you agree on specifications, budget and deadlines in advance. During the application development you keep your buyer up-to-date, but you don't need to negotiate further.

### Flexible

More flexible models are Time & Material or Dedicated Team contracts. These are especially suitable for relatively complicated projects. You and your buyer discuss and agree on the specifications of the application during the development process. This also means the budget and deadlines are not set in advance. These types of contracts require intense communication with your buyer.

### Tips:

Listen carefully to your buyer's ideas, problems and wishes and thoroughly document them. Ask questions to better understand what your buyer wants.

Be in regular contact with your customer about the progress you are making.

Be prepared to communicate with your buyer during their office hours, even if they are in a different time zone.

If you use a fixed price contract, make clear agreements with your buyer on a structured plan and the expected timeline of the project.

For more information on the different types of contracts, see Cleveroad's [Types of Contracts](#) in

### 3. Which European markets offer opportunities for information security application development?

#### Increased spending on information security

[Internet security threats are numerous and continue to increase](#). In 2017, there were up to nearly one million web attacks against people every day; one in every 13 web requests led to web addresses with malware. In addition, most legitimate websites have unpatched vulnerabilities that put millions of users at risk.

Other information security threats on the rise as of 2017, in contrast with 2016, include:

- 8.7 million malicious mobile apps blocked, with 54% more new variants
- 50,000 attacks on Internet of Things devices, a 600% increase
- 212 recorded vulnerabilities in industrial control systems, a 29% increase
- 1242 ransomware detections per day, with a 46% increase in new variants

As a result, [global information security spending grew from €88 billion in 2017 to €99 billion in 2018](#). This average annual growth of 12% is [double the rate of overall IT spending](#). In 2019, spending is forecast to grow a further 8.7% to €108 billion. Western Europe is the second largest market for security spending after North America.

The market is expected to continue growing, as security technology must keep up with constantly evolving threats and security requirements. Europe's new [General Data Protection Regulation](#) is also a key driver for companies to increase their information security spending.

#### Tips:

Focus on Western European countries, as security spending is highest there.

Stay up-to-date on hacker tactics and vulnerabilities.

Research the information security application market in your target country to optimise your offer. For example:

Study websites of local information security service providers for insights into buyer requirements and current offerings.

Check websites of trade associations and magazines for insights into market trends and developments.

Attend relevant industry events to meet potential buyers and find out their needs.

#### Smaller companies must increase their information security

All vertical markets are vulnerable to security breaches. Security spending is increasing rapidly, especially in healthcare and ICT. The [sectors with the highest information security spending](#) in the coming years are:

1. banking
2. discrete manufacturing

### 3. government

Large companies have the highest budgets for information security measures. They are relatively interesting targets because they are a vast source of information for hackers to exploit, sell or use for economic gain. For example:

- trade-strategy documents
- intellectual property related to product design
- large volumes of consumer data

As larger companies continue to up their security measures, [hackers increasingly target smaller companies](#). Many small to medium-sized enterprises (SMEs) don't have security measures in place that match the maturity of large companies. This means smaller companies also offer good opportunities for you.

#### **Tips:**

Focus on a sector with high or increasing security spending.

Offer customised information security applications for large companies or SMEs.

The [top 10 information security threats to European companies](#) are:

1. malware
2. web based attacks
3. web application attacks
4. phishing
5. spam
6. distributed denial of service (DDoS)
7. ransomware
8. botnets
9. insider threat (malicious or accidental)
10. physical manipulation, damage, theft and loss

To deal with these, the [top information security spending priorities for European companies](#) are:

1. data loss prevention — 55%
2. email security, encryption and endpoint security — 52%
3. identity and access management (IAM) — 42%

[The new General Data Protection Regulation](#) may further stimulate spending on IAM to manage data of individuals in the European Union.

#### **Tips:**

Keep up-to-date on the main information security threats to European companies.

Provide services/solutions that are in line with the top spending priorities.

## 4. What trends offer opportunities on the European market for information security applications?

### Increasing use of mobile devices

The European market for mobile devices continues to perform strongly. [The number of European smartphone subscriptions is expected to grow by 4–11% per year](#) between 2016 and 2022. The data traffic per smartphone in this period is predicted to increase by up to 42% annually. In 2015 already, around 90% of European households owned a smartphone and around 60% owned a tablet. These mobile devices are driving demand for mobile applications.

Keeping up with this trend, [29% of European organisations plan to investment in mobile security](#). This is an increase of 26% in comparison with 2017.

[European spending on mobile applications \(including user spending and advertising\) amounts to 30% of the global market](#). It totalled €6.1 billion in 2013 and is estimated to reach €18.7 billion by 2018. Most of this spending comes from Northern and Western Europe. [Users in Northern and Western European countries are expected to download more than 33 billion apps in 2019](#).

#### Tips:

Provide information security applications for mobile devices, both for the consumer and the business market.

Focus on Northern and Western European countries, as mobile application spending is expected to be highest there. These countries are relatively open to international services outsourcing.

### Internet of Things becoming mainstream

The Internet of Things is on the rise. It consists of (even everyday) objects that are connected to the internet. There could be as many as [20 billion connected “things” by 2020](#), with about [6 billion of them in Europe](#). The Internet of Things is an increasing security concern, for example because hackers can use these connected devices in DDoS attacks. According to AT&T, [35% of companies in Europe, the Middle East and Africa \(EMEA\) don't have confidence in the security of their own connected devices](#).

#### Tips:

Offer information security applications related to the Internet of Things.

For more information, see our study on the [Internet of Things](#).

### Technological developments drive interest in holistic security approaches

Holistic security operates on multiple, fully integrated levels for an entire organisation. It considers a company's system as a whole to achieve maximum security. It combines:

- security technology (software)
- security procedures
- people working within the system

Technological developments, like the Internet of Things and the big data sets it creates, require more complex data security systems. This increased complexity and digitisation of life continues to drive the interest in holistic security.

### **Tips:**

Provide holistic information security applications, especially if you target companies that work with large volumes of data. For example to prevent data loss with both network-level and endpoint-level controls.

For more information, see our study about [big data](#).

## **Online financial transactions increasing**

The number of online transactions continues to increase. For example, [the European ecommerce industry is estimated to have reached €602 billion in the end of 2017](#). This is a growth of 14% compared to the previous year. After overtaking desktop in 2017, [mobile is now the leading platform for online transactions with 52% of the market](#). Online payment is especially popular in Northern and Western Europe. These financial transactions need to be secure. Their increase drives demand for financial information security applications.

### **Tips:**

Offer financial information security applications for browser and mobile transactions.

Focus on Northern and Western European countries.

See our study about [trends on the European outsourcing market](#) for more information on general trends.

## **5. What requirements should information security services comply with to be allowed on the European market?**

### **What legal and non-legal requirements must you comply with?**

#### **General Data Protection Regulation**

Europe's new [General Data Protection Regulation](#) (GDPR) has come into effect on 25 May 2018. This regulation is designed to protect individuals in Europe from privacy and data breaches. Under the GDPR, any company or individual that processes data is also responsible for its protection. It applies to all companies processing the personal data of persons in Europe, regardless of the company's location. This means it also applies to you directly.

The personal data this regulation protects can range from a name or email address, to bank details, social media content, a photo or an IP address. Some key consumer rights you must comply with include consent, right to access, data portability and the right to be forgotten. You also need to practice privacy by design, meaning data protection should be included from the onset of designing systems.

### Tips:

If you process data of people in the EU, regardless of where you are in the world, make sure you comply with the GDPR.

For more information on the GDPR (and other European legislation), see our study about [buyer requirements on the European outsourcing market](#).

## Copyright - Legal protection of computer programs

The European Union has established specific rules to protect computer programs by means of copyright.

The [Directive on the legal protection of computer programs](#) (2009/24/EC) establishes that:

- you have to make sure not to breach any copyright when placing your computer programme on the market
- your products are also protected against unauthorised reproduction

### Tip:

Read more on the [legal protection of computer programs](#) on the website of the European Commission.

## What additional requirements do buyers often have?

### Voluntary data security ISO standards

Data security is one of the main challenges for service providers. This includes both data protection and recovery systems. Many European buyers expect you to have information security and management systems in place. Especially in industries where security is essential, such as finance and banking or mobile applications. The [ISO 27000-series on information security](#) contains common standards.

### 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 27002 code of practice for information security](#).

See our study about [buyer requirements on the European outsourcing market](#) for more information.

## 6. What competition do you face on the European information security application market?

Competition on the European information security application market does not differ significantly from the outsourcing market in general. Refer to our [top 10 tips for doing business with European buyers](#).



## Nearshoring more popular than offshoring

European companies prefer to outsource services to providers within the same country (onshoring). When outsourcing abroad, they prefer nearshore locations because of:

- proximity
- language
- cultural similarities
- little or no time difference.

These are usually Eastern European countries, due to their relatively low wages. For example:

- Poland
- Bulgaria
- Romania

However, prices in nearshore countries are rising. This makes service providers in these countries less competitive for offshore service providers. That means you can either form subcontracting partnerships with them, or compete with them.

Offshoring destinations with the strongest potential are:

- India
- China
- Malaysia
- Indonesia
- Brazil
- Vietnam

### Tips:

Limit the possible disadvantages of being offshore. Provide excellent communication, availability in the required time zone and good security and privacy measures.

Differentiate yourself from onshore and nearshore providers to remain competitive. Emphasise how you are different in your marketing message. Do not only compete on price, but also analyse what other advantages you can offer. For example access to skills, specialised industry expertise or around-the-clock operations (24/7).

Research what your competitors are doing right and wrong. This can help you differentiate yourself from them.

Partner with nearshore service providers, as Eastern European companies are looking for cheaper destinations. Many service providers in developing countries have not yet recognised this opportunity.

## 7. Through what channels can you get your information security application services on the European market?

### Subcontracting by European service providers

Subcontracting by European service providers is one of your most realistic market entry channels. It means that European service providers subcontract information security application development assignments to you, that end user companies have contracted to them. These local service providers know the local market well and already have a customer network. Another advantage of subcontracting are the low up-front capital

investments.

### Tips:

Decide on a business model. Either develop your own information security applications, or focus on development services for a European partner.

Target service providers whose size is in line with your capacity.

Focus on companies that serve the same horizontal or vertical markets as your company.

Attend relevant industry events in your target country to meet potential partners. This also allows you to learn more about their business culture. For example the [Gartner Security & Risk Management Summit](#) and [Infosecurity Europe](#) in the United Kingdom, [CEBIT](#) and [IT-SA](#) in Germany and [ISSE](#) at various locations in Europe.

Use industry associations to find potential customers in Europe. For example [Bitkom](#) in Germany, [Nederland ICT](#) in the Netherlands and [UKITA](#) in the United Kingdom.

National outsourcing associations can also be interesting sources to find potential customers. For example [Global Sourcing Association](#) in the United Kingdom, [Outsourcing Verband](#) in Germany and [Platform Outsourcing](#) in the Netherlands.

Develop good promotional tools, such as a professional company website and a company leaflet. Also invest in Search Engine Marketing, so potential customers can easily find your company online.

## Direct sales to end users

You can also try to sell your information security services directly to end user companies. New electronic marketplaces may make this easier. These marketplaces are a cheap marketing tool. Although they mainly contain smaller projects for freelancers, they could lead to pilot projects for companies. However, you need excellent end market knowledge.

### Tips:

Research the end market segment that you want to focus on. This allows you to effectively market your company.

Look for potential leads in the field of information security application development on online outsourcing marketplaces. For example [UpWork](#) and [Freelancer](#) (freelancers), [Ariba](#) (corporate) and [LinkedIn](#).

## Intermediary

You can approach European service providers and end users of information security applications directly, or through an intermediary. A local contact person is an advantage, especially if you are located in a lesser-known outsourcing destination. Intermediaries, such as a consultant/matchmaker or sales/marketing representative, can therefore be an important channel to establish contact with potential buyers.

Refer to our study on [finding buyers in the European market](#).

## 8. What are the end market prices for information security applications?

Price is the main reason for companies in Europe to outsource information security application development to developing countries. Staff salaries make up a large share of the costs of IT services. This means outsourcing to countries with lower wages can lead to considerable savings. For example, the average annual salary of a software developer in Western Europe is between €36,000 and €50,000. In offshore destinations, this is usually significantly lower.


### Tips:

Research the average salaries for software developers in your European target country. For example via [Payscale](#), a global database for salary profiles.


Emphasise the potential salary savings in your marketing activities.

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](#)