HSP GROUP
Global Expansion Simplified

How Will the GDPR Data Privacy Law Affect Your Business's Global Expansion?

An 8-step guide to understanding GDPR and Technical Organizational Measures

TABLE OF CONTENTS

INTRODUCTION

Any business nowadays must factor in full legal compliance with the data privacy laws of the country or countries in which they operate. If you operate in one or more of the European Union (EU) Member States and/or the United Kingdom (UK), then the critical legal data compliance framework to which you must adhere is the '**General Data Protection Regulation**' (GDPR). In force since 2018, this complex data privacy law is known to be the world's strictest.

To achieve the GDPR's highly complex 99 Articles of Compliance requirements, it is crucial that your organization has the associated technical organizational measures (TOMs) in place, all of which require certain minimum infosec and technology standards.

While this eBook addresses GDPR compliance specific to the EU and the UK, note that, regardless of where your business operates, it will have a legal obligation to be compliant with the local regime. Non-compliance can result in severe penalties. There are countries all over the world with data compliance legislations similar to the GDPR, each of which shares common fundamental principles of data protection, a local regulatory approach, and penalties for non-compliance. For example, the '**California Privacy Rights Act**' (CPRA), in force since 2023, is closely modeled on many aspects of the GDPR.

The GDPR, however, is still regarded as the most stringent of all the world's data privacy frameworks and is also currently the most punitive and heavily regulated. Read further to learn about GDPR, its impact on your business's long-term success, and how you can successfully navigate the law's complex compliance requirements.

Paul Sutton
Director of Legal, HSP Group
Contact@hsp.com

GDPR COMPLIANCE

Which businesses must comply with GDPR?

Whether or not your organization has a business operating within the EU and/or the UK, you will still be required to comply with the GDPR (and associated TOMs) requirements if you collect/process the data of EU/UK residents.

Even if the data you collect is for an organization, for example, in the US, the GDPR still applies to you. That's because the law has what is called 'extra-territorial' jurisdiction—EU/UK regulators can pursue actions against organizations based anywhere in the world. Regulators can also enforce large financial penalties for non-compliance with the GDPR wherever EU/UK residents' data is processed if the non-EU/UK-based organization has not taken steps to be fully compliant with the GDPR.

For these reasons, it is essential that your organization has a good grasp of the GDPR and associated Technical and Organizational Measures (known as TOMs, these are the technology and organizational measures that you must have in place to ensure that the personal data you collect remains protected and secure). The GDPR applies to you if:
(1) you are a business looking to conduct business in one or more of the EU Member States and/or the UK or
(2) you have no business presence there, but you nonetheless collect/process the data of EU/UK residents while operating in another country (for example, the US).

Consequences of GDPR non-compliance

Failure to be able to demonstrate full compliance with the GDPR to the relevant national data regulator can be a costly mistake for your business. Non-compliance penalties with the GDPR can extend to EUR 20M or 4% of an organization's global turnover, whichever is greater.

Will you be caught for non-compliance?

Yes! These days, the relevant national tax authorities and other compliance agencies work very closely with data privacy regulators. If you are not in compliance with the GDPR, it is virtually impossible for you to avoid falling on the radar of the relevant data privacy regulator if you engage in business of any nature in that regulator's country.

Does your US-based business collect personal data from EU/UK residents?

Even if your US-based business doesn't operate in the EU/UK, if you collect personal data from EU residents, GDPR and its penalties apply to you. HSP's global experts have the full breadth of legal and regulatory knowledge to ensure that you stay compliant and avoid costly penalties.

Check out our **Technical Consulting Solutions** today, then **Contact Us** to start your GDPR compliance journey.

UNDERSTANDING THE GDPR

What does the GDPR cover?

In essence, the GDPR is EU/UK legislation that regulates the secure processing of the personal information (or personal "data") of individuals who reside in these countries. It is widely acknowledged as the toughest and most penal data privacy and security law in the world.

The role of Technical Organizational Measures (TOMs)

The key goal of TOMs is to ensure that your organization avoids data breaches and stays in compliance with all relevant data privacy obligations under the GPPR. In fact, the GDPR explicitly mentions TOMs more than 90 times. Specifically, TOMs are the designation given to the technology around the functions, processes, controls, systems, and procedures implemented to support the secure processing and storage of personal data. They also cover the relevant specific data privacy-related policies and other documents an organization must have prepared to ensure compliance with the GDPR.

Is your business considering international expansion?

A key part of a successful international expansion is compliance with the GDPR. HSP's team of global experts can give you peace of mind—**our team of experts** will navigate the complexities of the GDPR for you so that you can focus on what you do best—your core business.

Get in touch with us to find out how we can offer you a seamless path to GDPR compliance before you expand internationally.

THE CORE PRINCIPLES OF GDPR

The core principles of GDPR

1. **Lawfulness, fairness, and transparency**
   This principle requires that personal data be processed lawfully, fairly, and in a transparent manner. Organizations must have a legal basis for processing data, inform individuals about the data processing, and ensure that their processing activities are fair and just.

2. **Purpose limitation**
   Data should be collected for specified, explicit, and legitimate purposes. It should not be further processed in a way that is incompatible with these original purposes.

3. **Data minimization**
   Also related to the principle of purpose limitation, data minimization means that organizations should only collect and process data necessary for the specified purposes. Unnecessary data should not be collected.

4. **Accuracy**
   Organizations are required to ensure that the personal data they process is accurate and up to date. They should take reasonable steps to rectify or erase inaccurate data.

THE CORE PRINCIPLES OF GDPR

5. **Storage limitations**
   Personal data should be kept in a form that allows the identification of data subjects for no longer than is necessary for the purposes for which the data is processed. This principle encourages the deletion or anonymization of data when it is no longer needed.

6. **Integrity and confidentiality**
   This principle mandates that organizations take appropriate security measures to protect personal data from unauthorized or unlawful processing, accidental loss, destruction, or damage. It encompasses data security practices like encryption, access controls, and regular security assessments.

7. **Accountability**
   Organizations are themselves responsible for demonstrating compliance with the GDPR. This includes keeping records of data processing activities, conducting data protection impact assessments (DPIAs) when necessary, and appointing a Data Protection Officer (DPO) in certain cases. Accountability also includes an obligation to report most data breaches to the relevant national data regulatory authority and to cooperate fully with that authority as required.

Build compliance into your global strategy

GDPR compliance is not an option but a requirement. In fact, non-compliance can result in severe penalties (up to EUR 20M or 4% of global turnover), damage to your company's reputation, and costly legal repercussions.

Contact HSP's global experts today to ensure that you proactively, seamlessly, and effectively build compliance into your global expansion strategy.

EXAMPLES OF DATA BREACHES

Common examples of data breaches

To put the importance of GDPR into context (and to demonstrate how easy it can be for any organization to slip up and cause a data regulatory breach that could result in an expensive fine), here are some examples of the most common breaches of the GDPR. These examples go beyond the GDPR—they apply equally to any other data privacy framework elsewhere in the world:

Emailing personal data to the wrong address

An organization sends an email containing personal data to the wrong email address despite having the correct email address on file. This is considered the single most common cause of data breaches. A moment's lack of concentration by an employee in sending an email can cause a minefield of regulatory investigation for an organization and possibly a very penal fine. The fine imposed would be considerably higher if the organization was found not to be fully compliant with the GDPR in terms of its relevant policies and other relevant documentation and its TOMs generally.

Improper disposal of personal data

A company fails to correctly dispose of paperwork (or software) containing personal data, meaning an unauthorized person might access it. This, again, is a very common cause of complaints by a 'data subject' (i.e., the individual whose data has been put at risk).

Vulnerability to ransom ware

A company falls prey to cybercrime via a ransom ware attack. If an organization fails to update its online security systems, it might be vulnerable to a ransom ware attack. This may result in cybercrime and the theft of personal data. This type of data breach is becoming increasingly common and would lead to an intensive investigation by the relevant regulatory authority. That's why it is critical that an organization ensures that its TOMs are adequately compliant from a regulatory perspective and are reviewed on a regular basis.

How preventable is GDPR non-compliance for your organization?

If you don't fully understand the GDPR and/or lack the measures in place for compliance, data breaches occur more easily than you think. And, because regulatory authorities are increasingly vigilant, it's nearly impossible for your businesses not to fall under the radar if that is the case. **Check out our blog** for real-life examples of data breaches (including Meta's much-publicized GDPR rule-breaking incident). If you want peace of mind for your data security, **get in touch with us** today!

THE IMPACT OF GDPR AND TOMS ON BUSINESSES

How do GDPR and technical organizational measures affect a business's viability?

Organizations that process personal data (essentially ANY organization doing business of any nature, regardless of how large or small) MUST integrate GDPR compliance principles into their data handling practices and privacy policies.

In addition to reputational damage, companies that fail to adhere to GDPR regulations can face financial penalties steep enough to derail the stability of the business—even a penalty of much less than the maximum (EUR 20M or 4% of turnover if greater) can be catastrophic.

Compliance with these GDPR principles and the associated TOMs is essential for organizations to be able to demonstrate that they 'adequately' (a term used in the GDPR) protect an individual's privacy rights.

Which steps should you take to protect your business' global expansion goals?

The sheer complexity of GDPR, with its 99 articles and numerous requirements, is extremely difficult to navigate in-house for most companies. And yet, mitigating risk in a complex global regulatory environment is necessary for your long-term success.

Our experts are well-versed in the complex global regulatory landscape, from GDPR and beyond. **Contact HSP** today for a solution tailored to your business's global expansion needs.

ADVANTAGES OF OUTSOURCING GDPR COMPLIANCE

Advantages of outsourcing GDPR and related considerations

To help businesses put the necessary steps in place to ensure compliance with the GDPR (and/or any other relevant data privacy framework for countries outside the EU/UK), consider outsourcing this complex area of compliance to experts who can create a tailored solution to your business's specific needs and expansion goals. From drafting policies to advising your HR and other teams on the practicalities of ensuring internal compliance, experts can help alleviate the burden of staying abreast of changing regulations and requirements.

Here are three reasons to consider outsourcing GDPR compliance:

1

Reduce the burden on your internal HR team: Businesses' legal obligations regarding data privacy laws, especially the GDPR and its associated TOMs, are complex and ever-changing. The sheer complexity of GDPR, with its 99 articles and numerous requirements, is extremely difficult to navigate in-house for most companies, requiring specialized expertise, real-world experience, and an ongoing commitment to staying abreast of the changing regulatory landscape.

2

It's relatively easy to fall out of compliance: The potential consequences of non-compliance, such as substantial fines (up to EUR 20M or 4% of global turnover), are not worth the risk of falling out of compliance. Because regulatory authorities are increasingly vigilant, it's nearly impossible for non-compliant businesses to not fall under the radar (and remember, common GDPR breaches occur more easily than you think).

3

Mitigate risk to ensure your company's success in global expansion: Staying compliant with GDPR can have an outsized impact on your company. Mitigating risk in a complex global regulatory environment is necessary for your long-term success. Remember, not only does GDPR compliance apply to US businesses (if they collect/process data of EU/UK residents), but similar data privacy laws are also emerging worldwide, thereby increasing complexity and risk.

Focus on what you know best—your core business.

By outsourcing to a company with proven GDPR and compliance expertise, you'll have immediate access to expert regulatory, infosec, and technical expertise. You'll also have the peace of mind that you'll always be up to date on regulatory changes and the flexibility to receive whatever support you need as your company or the global environment changes.
Focus on what you know—your core business—by leveraging the experts uniquely positioned to implement GDPR compliance thoroughly and cost-effectively across your entire organization. **Contact us today to get started.**

DO YOU NEED HELP MANAGING GDPR AND TOMs?

Do you need help managing the GDPR and Technical Organizational Measures?

HSP has a dedicated team of expert specialists who work with customers on data privacy compliance and related matters. They have in-depth experience advising on data privacy in over 140 countries from both a regulatory and a practical implementation perspective.

To find out more about how HSP could help you with GDPR and its related Technical Organizational Measures, **contact an HSP expert today to get started on your successful global expansion journey.**