Privacy challenges of expanding your business to and within the EU

Privacy challenges you will be facing

Scale-ups and start-ups face all kinds of different challenges while rapidly changing and expanding, such as dealing with growing workforce, ad-hoc processes, cash flow control, growing customer needs, and let us not forget compliance. This article focuses on how to approach setting up a privacy compliance program with limited financial and human resources and attempts to explore practical, efficient and scalable solutions on how to approach challenges.

liance

Kim van Assendelft
is a manager at KPMG Cyber & Privacy.

Disclaimer: this article cannot and shall not be regarded as legal advice. The content therein shall be regarded purely as the personal and professional opinion of the contributors.

INTRODUCTION

After more than 4 years of GDPR enforcement, complying with the GDPR and the related privacy standards still remains a challenge. That holds true both for companies established within the EU and maybe even more so for those that want to expand to the EU. Developing a business in the current social and economic landscape is certainly not an easy journey. Ensuring a privacy-compliant business only adds to the task. At the same time, the world is becoming more digitalized, with a considerable increase in development and usage of digital technologies having data at their core. This renders privacy even more important than ever. If bigger companies are more or less equipped with the necessary tools and FTE capacity and already way ahead in the process of GDPR compliance, for start-ups and scale-ups the GDPR compliance challenge is only at its rise.

This article focuses on exploring the GDPR compliance adventure from a start-up/scale-up perspective. Why? Because scale-ups and start-ups encounter all kinds of different challenges while rapidly changing and expanding, such as dealing with growing workforce, ad-hoc processes, cash flow control, growing customer needs, and let us not forget compliance. Whether your company is a scale-up or start-up in the EU with the ambition to expand within the EU or a scale-up or start-up for example in the US with the ambition to expand to the EU, this article emphasizes GDPR compliance challenges for both. Furthermore, it attempts to explore practical, efficient and scalable solutions on how to approach the listed challenges.

Scale-up and start-ups have to be very creative when it comes to efficiently and effectively implementing a compliance program, they are often driven or distracted by everyday humdrum and lack resources, knowledge and cashflow. A comprehensive privacy compliance

program covers every data-privacy related requirement and provides your organization with a framework for processing, collecting, storing, sharing, retaining and deleting personal data. In this context, executing the entire compliance program and being fully compliant seems like quite the ambition. In reality, start-ups and scale-ups are very dynamic and fast growing, standardized processes are usually not implemented and happen with a rather ad-hoc approach. Furthermore, privacy projects are rarely on the top of the list of priorities when it comes to budgeting. At the same time, customers are becoming increasingly aware of their privacy and rights. Therefore, providing a great product or service to customers also means ensuring adequate levels of personal data protection. Besides, a GDPR fine can be devastating for already financially struggling starts-up and even scale-ups. So not complying with privacy laws is simply not an option.

The purpose of this practical article is to explore the main challenges for scale-ups/start-ups to achieve and maintain GDPR compliance so that the company can grow and expand rapidly. The identified challenges will be explored from the perspective of an EU-established company as well as a US-established company, both with the aim of expanding within the EU. This article is structured as follows:

- Everything starts with awareness
- Make sure you've got your priorities right
- Is your management on board?
- Key considerations for business expansion to different countries within the EU

Privacy is a team sport, it cannot be achieved by your Privacy Officer alone

EVERYTHING STARTS WITH PRIVACY AWARENESS

So, where to start? A scalable and solid compliance program starts with awareness. The data privacy landscape is very complex, and it continues to evolve, with a lot of new legislative proposals from the EU just around the corner ([EC]). In this context, it is critical that your employees know how to handle personal data in a privacy responsible and compliant manner. Privacy is a team sport, it cannot be achieved by your Privacy Officer or team alone. Aside from the fact that training your staff is an obligation imposed by the GDPR, the overall success of your company's privacy compliance is directly related to how much your employees care and understand privacy, why it is so important and how to address regulatory requirement internally. You cannot engage your employees and ask them to follow and implement legally required privacy standards if they do not understand or know how to determine personal data and how the GDPR affects this data. Therefore, for a strong foundation of your future compliance framework, focusing on awareness is the key. Although we now focus on training and awareness specifically related to privacy, it does not have to be addressed in a vacuum. Privacy trainings can be combined with other topics, such as security, integrity, or compliance.

Of course, awareness should be implemented with the GDPR basics ('Privacy 101'). Although GDPR has been around for a while now, do not assume that everyone knows what it entails. Therefore, first focus on creating a generic privacy training for all employees or leveraging existing training material. Focus on the topics that are relevant for all employees regardless of whether they handle personal data. Think of data breaches and how to recognize and report (internally), what does personal data and its processing entail and why it is important to comply with the GDPR. And don't forget to address the key GDPR privacy principles, such as transparency and data minimization. The purpose of the training is to create a shift in their mindset to critically think about why personal data is needed before processing personal data. GDPR is already perceived as a heavy topic, so try to make it fun and relevant.

Basics are good, but that is not enough. Therefore, as a next step you could focus on specific training for employees that are handling personal data or have responsibilities relating to processing personal data. Depending on your company, the focus could be on Sales, Marketing, Procurement, IT and Human Resources.

In this training, move a step ahead from the basics. Get your colleagues' attention by sharing practices with

them that are relevant for their daily activities. Also, share with them concrete information that is required for the specific teams to understand their responsibilities. For example, Human Resources should be made aware how to handle (former) employee data and data from applicants, and Procurement should be informed about the ins and outs of data processing agreements. And again, make it pleasant and convenient, for example, by inserting game elements in your training or making it interactive by including statements to start a discussion.

Besides traditional training, you need to find ways to make sure privacy is 'top of mind' within the company. You can do that by organizing various other initiatives. Send a newsletter when there is a breach that might be relevant to your company.

Awareness is not only about the once-a-year training, is it a constant and continuous effort that can have severe consequences if missed.

MAKE SURE YOU SET YOUR PRIORITIES

Next to awareness, it is important to set your priorities. Considering that limited FTE capacity is working on GDPR compliance, it is necessary to first think about your GDPR compliance strategy and determine the organization's risk profile and appetite. This will help you set the right priorities. Your risk profile and appetite may vary, for example your company may operate business-to-business or business-to-customer or your company may need to process more sensitive personal data.

Setting your priorities will not work without first understanding your data and risks. For that, you need to gather all relevant information, such as business plans or blueprints, and stakeholders to determine what the data will be used for and to determine the GDPR strategy and risk tolerance given the regulatory landscape. When assessing the risk appetite, take into account what your company likes to achieve with personal data and to communicate this externally, what role does personal data play in achieving the goals and milestones and the risk that your company is willing to take to achieve their goals effectively and efficiently. This can be used as input for the approach or GDPR program to implement.

Implementing a pragmatic approach will help to structure privacy tasks and activities and help prioritize compliance tasks and give some guidance. For example, you can adopt a generic framework, such as NOREA or NIST, and use that to make sure all your privacy tasks and activities are covered and tailor it to suit your company's needs. To tailor it, use the input from the strategy and risk profile and appetite taking into account the company's need and the legal environment.

Setting your priorities will not work without first understanding your data and risks

To help determine your risk appetite and profile, the first step is to gain an understanding of the processing activities by holding a data inventory or by registering processing activities.. This might look like a boring and redundant task for your manager, but it is a crucial step in establishing a strong relationship with your company. The register of processing activities contains details about what personal data the company holds, for what purposes, from which data subjects (customers, employees, business partners, etc.) and more. The register should be centered around processes, divided between the different departments or business activities within your company rather than based on individual IT systems alone. In line with your company's business goals and growth ambition, you are able to assess the risks that arise from processing personal data within your company and what activities to focus on.

To make it even more concrete. If you are a business-to-business company, you would probably focus more on employee data, since your company does not hold (or hardly) any customer data. If your company is a tech innovation start-up working with AI or other new technologies, you should focus more on the personal data processed by those technologies.

Now that you have set your priorities, you need to start executing. However, privacy projects are rarely on the top 3 items of the budgeting list within a start-up/scale-up, so one of the key success factors is the buy-in of your management, which will be addressed in the next section.

IS YOUR MANAGEMENT ON BOARD?

When defining your privacy priorities, make sure you include engaging your management into the company's privacy compliance journey as a priority to get broader and company-wide buy-in. That is usually a challenging task, as privacy is not a revenue generating source. So how can you bring your management on board? First, it is good to emphasize the fines that the GDPR imposes for non-compliance. Simply put; privacy does not bring your company any immediate financial benefits nor revenues, but it can clearly safeguard your company's budgets which can be severely impacted by a privacy fine. A fine imposed for GDPR non-compliance can have a tremendous impact on the whole existence and development of your company. Furthermore, you clearly do not want to have your newly established company in the news, under a GDPR fine headline.

Secondly, studies are showing that customers are becoming increasingly aware of their personal data. So being privacy compliant only adds value to your marketing strategy and can clearly provide a competitive advantage. Data privacy and security issues aren't just a matter of checking the compliance box; they have become strategic competitive advantages that can raise the bar on brand trust with consumers and employees.

KEY CONSIDERATIONS FOR BUSINESS EXPANSION TO DIFFERENT COUNTRIES WITHIN THE EU

Although the GDPR is intended to harmonize privacy laws and enforcement in Europe, you have to take into account the differences in privacy regulations between European Member States when the company would like to expand. Most Member States have introduced their own national legislation based on certain exceptions provided by the GDPR, for instance when it comes to national identifiers and the age of minors. Next to that, not only privacy laws are relevant, but also other national laws and (industry sector) regulations. For example, national employment laws could have an impact on the way personal data of your employees that is processed.

Secondly, besides making sure you adapt your practices to different national laws, you also need to make sure you keep up with all the legislative developments at the EU level, such as the enactment of the EU Data Act, the Data Governance Act and upcoming legislation such as the ePrivacy Regulation, the Digital Market Act, Digital Services Act and the AI Act. In an attempt to address all the challenges imposed by the new digital interactions between customers and businesses, EU institutions are working hard on adopting more robust standards for data protection practices, as well as increasing accountability from businesses engaging in such practices.

For example, before expanding to the EU, you need to think about the location of your headquarters. If you are a US-based company willing to expand to Europe, you will encounter differences in the implementation of the GDPR; the one that stands out the most is probably the enforcement by Member States' Data Protection Authorities. Every Member has its own Data Protection Authority governing the implementation of the GDPR. In this regard, when your company considers expanding within the EU, you will likely stumble upon deviations in regulations when it comes to privacy. As mentioned, this has to do with the freedom that the GDPR leaves for national choices, as well as national law that can exist alongside the GDPR and, for example, has stricter requirements regarding the processing of personal data of employees or the processing of the social security number. The aforementioned challenges show that your company's business expansion strategy must also be determined in accordance with applicable privacy requirements.

CONCLUSION

A start-up or scale-up is characterized by a rapidly changing and expanding environment, often facing many challenges. Given that GDPR is not always a top priority, scale-ups and start-ups have to be very creative when it comes to efficiently and effectively implementing a compliance program, they are often driven or distracted by everyday humdrum and lack resources, knowledge and cashflow. A pragmatic privacy program, setting the right priorities, ensuring buy-in and having privacy aware employees can help effectively tackle these challenges.

Reference

[EC] European Commission (n.d.). A Europe fit for the digital age. Retrieved from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

About the author

Kim van Assendelft is a manager at KPMG Cyber & Privacy and has experience as a Privacy Officer for a scale-up in the Netherlands and advisor for a start-up in the US with the ambition to expand to the EU.

This article was created in collaboration with Valentina Rosca, former DPO of felyx, a scale-up located in the Netherlands.