LOG206: E-Business

Spring 2018

Notes

Module 3: Macro environment of digital business

Introduction

Everyday the market for digital business is changing the way it is. Many new things are developed and circumstances are constantly changing. Among ythese, are things that greatly influence us but they are beyond our control. Digital businesses are also influenced by the factors in their external environment. The environment that surrounds the digital business is complex and constantly changing, as a result digital businesses are constantly presented with new opportunities and challenges. Therefore, it is imporatnt to keep track and constantly analyze the environment in which they operate.

SLEPT Analysis

SLEPT analysis is a framework to assess an organization's external environmental influence on it. It considers five factors affecting the macro-environment - Social, Legal, Economic, Political and Technological (hence the mnemonic SLEPT). The outcome of SLEPT analysis is an overall picture of the macro environment to identify threats and opportunities. SLEPT helps to identify and hence take advantage by maximizing opportunities and minimizing threats. It gives an understanding of the broad and long term trends and makes the firm in a better position for strategic decision making.

Sociological

Sociological attitudes and profiles are constantly changing. Developing a demographic profile of your consumer base will help you understand what motivates them. Keeping abreast of issues such as gender bias, ethnic origin and religion, as well as being conscious of social norms and lifestyle expectations, can help you with your marketing strategy.

Legal

Businesses across the world operate in a web of legal obligations and restrictions. Some of these relate to internal obligations such as those dealing with health and safety, while others have a wider impact on matters as diverse as waste and environmental management, import and export restrictions and or consumer protection laws. As part of your SLEPTanalysis, you should develop a broad knowledge of all legislation that impacts your business to minimize the risk of non-compliance leading to litigation.

The new EU data protection framework

The EU adopted the new data protection framework on 8 April 2016 which shall regulate the processing by an individual, a company or an organisation of personal data relating to individuals in the EU. The framework, which is called the General Data Protection Regulation (GDPR), will take effect on 25 May 2018.

Key aspects of the GDPR

1. Expanded territorial reach
   The GDPR catches data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behaviour of, EU data subjects (within the EU). In practice this means that any company outside the EU which is targeting consumers in the EU will be subject to the GDPR, which is not the case currently.

2. Data controllers, data processors, and data protection officers
   As a data controller, your company/organization will be responsible for determining the purposes for which and the means by which personal data is processed. Employees processing personal data within your organisation do so to fulfil your tasks as data controller. Your company/organisation is a joint controller when together with one or more organisations it jointly determines 'why' and 'how' personal data should be processed

   The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.

   Your company/organization, whether it's a controller or a processor, needs to appoint a data protection officer (DPO) if its core activities involve processing of sensitive data on a large scale or involve large scale, regular and systematic monitoring of individuals. In that respect, monitoring the behaviour of data subjects includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. Public administrations always have an obligation to appoint a DPO (except for courts acting in their judicial capacity).The DPO may be a staff member of your organisation or may be contracted externally on the basis of a service contact. A DPO can be an individual or an organisation.

   The DPO assists the controller or the processor in all issues relating to the protection of personal data. In particular, the DPO must:
   - inform and advise the controller or processor, as well as their employees, of their obligations under data protection law;
   - monitor compliance of the organisation with all legislation in relation to data protection, including in audits, awareness-raising activities as well as training of staff involved in processing operations;

- provide advice where a DPIA has been carried out and monitor its performance;
- act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights;
- cooperate with DPAs and act as a contact point for DPAs on issues relating to processing

3. Accountability and privacy by design
   The GDPR places onerous accountability obligations on data controllers to demonstrate compliance. This includes requiring them to: (i) maintain certain documentation, (ii) conduct a data protection impact assessment for more risky processing (DPAs may compile lists of what is caught), and (iii) implement data protection by design and by default, eg data minimisation.

4. Role of data processors
   One of the key changes in the GDPR is that data processors have direct obligations for the first time. These include an obligation to: maintain a written record of processing activities carried out on behalf of each controller; designate a data protection officer where required; appoint a representative (when not established in the EU) in certain circumstances; and notify the controller on becoming aware of a personal data breach without undue delay. The provisions on cross border transfers also apply to processors, and BCRs for processors are formally recognised.

5. Consent
   Consent must be freely given, specific, informed and unambiguous. Requests for consent should be separate from other terms, and be in clear and plain language.
   A data subject's consent to processing of their personal data must be as easy to withdraw as to give. Consent must be "explicit" for sensitive data. The data controller is required to be able to demonstrate that consent was given. Existing consents may still work, but only provided they meet the new conditions.

6. Transferring data outside the EU
   In today's globalised world, there are large amounts of cross-border transfers of personal data, which are sometimes stored on servers in different countries. The protection offered by the General Data Protection Regulation (GDPR) travels with the data, meaning that the rules protecting personal data continue to apply regardless of where the data lands. This also applies when data is transferred to a country which is not a member of the EU (hereinafter referred to as 'third country').

   The GDPR provides different tools to frame data transfers from the EU to a third country:

   Sometimes, a third country may be declared as offering an adequate level of protection through a European Commission decision ('Adequacy Decision'), meaning that data can be transferred with another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions.

In other words, the transfers to an 'adequate' third country will be comparable to a transmission of data within the EU.
in the absence of an Adequacy Decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Such appropriate safeguards include:

- in the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on so-called binding corporate rules;
- contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission;
- adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.

Finally, if a transfer of personal data is envisaged to a third country that isn't the subject of an Adequacy Decision and if appropriate safeguards are absent, a transfer can be made based on a number of derogations for specific situations for example, where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer.

Economic factors

The strength and performance of the local, national and international economy can all impact a business, presenting both opportunities and threats. Different types of taxation and other duties can also hit your bottom line hard, so a deep understanding of the fiscal environment is essential in order to prepare viable financial forecasts. The economic health and competitive environment in different countries will determine the e-commerce potential of each. Managers developing e-commerce strategies in multinational companies will initially target the countries that are most developed in the use of the technology.

Political factors

Political factors include how regulations and policies imposed by your national or local government might affect the way you conduct your business. For example, import and export tariffs may make it difficult or uneconomical to do business with certain countries. At a local government level, there may be restrictions on the kind of businesses permissible in certain locations, while in certain sectors of the economy, lobbying may be more or less prevalent.
The political environment is shaped by the interplay of government agencies, public opinion, consumer pressure groups such as CAUCE (the Coalition against Unsolicited E-mail), www.cauce.org, and industry-backed organizations such as TRUSTe (www.truste.org) that promote best practice amongst companies. The political environment is one of the drivers for establishing the laws to ensure privacy and to achieve taxation.

Technological factors

The only thing permanent about technology is change. With advances in technology developing at a seemingly unstoppable rate, keeping up-to-date with changes could help you develop a

market advantage in the face of competition. As a business manager, you should look at ways to harness technological potential to identify and service new and emerging markets. One of the great challenges of managing digital business is the need to be able to assess which new technological innovations can be applied to give competitive advantage.

Evaluating business models' robustness

Apart from viability and feasibility, a successful business model must also be robust. The feasibility of a business model is checked by the narrative test and the number test explained in the previous module. Robustness of a business model is concerned with the long-term viability and feasibility of a BM in a given future environment. It is important to systematically evaluate business models against potential threats and opportunities since the future of a business model is too important to be left to random chance and guesswork. Evaluating the robustness of a BM in an uncertain business environment can be done by business model stress testing.

Business Model Stress Test

The Business Model Stress Test helps you to understand if your business model is future proof. Changes in markets, society and technology might impact your business model in the future for which you can prepare with this tool. With the Stress Test you can analyse the strong and weak parts of your business. It helps you to find opportunities for making your business more robust.

Performing Business Model Stress Test

In a Business Model Stress Test you confront a business model with relevant developments and uncertainties in politics, economy, society, technology, market or regulation. Some trends are quite certain, like the ageing population, while other developments are uncertain, like the economic environment. For selected developments we assess the impact on the business model and identify the business model's strong and weak parts in a heat map. By following the steps below, you will be able to complete the Business Model Stress Test:

Step 1: describe the business model

Describe your current or future business model in a structured format, for example using the nine components of the Business Model Canvas or any other sensible framework. This will enable you to systematically test your business model's components against future trends and uncertainties.

Step 2: select the essential scenarios

Select the most relevant developments (trends and uncertainties) in technology, market, society and regulation that may have an impact on the business model. You may gather these developments from a SLEPT analysis. However, many relevant developments can also be found in trend- and scenario reports or industry analyses that are freely available on the internet. Naturally, the uncertainties have multiple possible outcomes. You must consider the possible 'extreme' outcomes and include them in the Stress Test.

Step 3: confront the business model with the scenarios

Now it is time to confront the business model components - e.g. value proposition, customer segments and revenue model - with trends and uncertainties. How does your business model fit with these future developments, or how is it impacted? In the stress test you confront each business model component with each development in a 'heat map'. Use a colouring scheme to indicate the impact of an uncertainty outcome on a BM element Use a green colour if the impact is clearly positive – the development is favourable for your business model. Use red colouring if a development has an obvious negative impact and may cause great problems to your business model. Use orange to indicate that a business model component requires attention due to certain development. If a development has no impact, then you don't need any colouring. Once the stress test is completed, the heat map will reveal the strong and the weak parts of your business model. The red parts indicate critical issues that need attention and the orange parts require at least some attention. It is important to write down why a development is positive, negative or requires attention. This provides insights in the reasons behind the strong and weak parts and may provide clues as to how to strengthen the business model.

Step 4: analyse and improve

In this step you analyse the heat map. Where are the weak points and what adaptations can be made to improve the business model and make it more robust? The arguments that you have listed when doing the stress test can be used as clues towards formulating concrete actions that could help you to improve your business model further.

References

Business Makeover. (2016). The Business Model Stress Test. Retrieved December 30, 2017, from https://www.businessmakeover.eu/platform/home/

Chaffey, D. (2015). Digital Business and E-Commerce Management - Strategy, Implementation and Practice. Chapter 4.

EU (2017). General Data Protection Regulation GDPR. https://gdpr-info.eu/

Haaker, T., Bouwman, H., Janssen, W., & de Reuver, M. (2017). Business model stress testing: A practical approach to test the robustness of a business model. Futures, 89, 14–25. http://doi.org/10.1016/J.FUTURES.2017.04.003