DIGI-GRENT Project

Good practice

Date:	04.10.2019
Place:	Thessaloniki, Greece

Authors

No.	Name and Surname
1	**Apostolos Pezodromou**
2	**Kirill Medovshchikov**

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1 Introduction

1.1 Good practice definition

Good practice is a method or technique that has been generally accepted as superior to any alternatives. It has been proven to work well and produce good results[1].

1.2 Good practice criteria

The following set of criteria will help you to determine whether a practice Is a 'good practice':

- ***Effective and successful***
  A good practice has proven its strategic relevance as the most effective way to achieve a specific objective; it has been successfully adopted and has had a positive impact on individuals and/or communities.
- ***Digitally-driven or digitally-enabled***
  A good practice that uses technology (digital means) in order to ensure its operations, innovation or collaboration.
- ***Environmentally, economically and socially sustainable***
  A good practice meets current needs, in particular the essential ones of the world's poorest, without compromising the ability to address future needs.
- ***Technically feasible***
  Technical feasibility is the basis of a good practice. It must be easy to learn and implement.
- ***Inherently participatory***
  Participatory approaches are essential, as they support a joint sense of ownership of decisions and actions.
- ***Replicable and adaptable***
  A good practice should have the potential for replication and should therefore be adaptable to similar objectives in varying situations.
- ***Reducing disaster/crisis risks, if applicable***
  A good practice contributes to disaster/crisis risk reduction for resilience.

[1] Nash, J. and Ehrenfeld, J., (1997), "Codes of environmental management practice: assessing their potential as a tool for change." Annual Review of Energy and the Environment 22, pp. 487-535; Bretschneider, S., Marc-Aurele, F.J., Jr., and Wu, J. (2005), "Best Practices" Research: A methodological guide for the perplexed, Journal of Public Administration Research and Theory , (15) 2, pp. 307-323.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2 Good practice description

The good practices for the training in Thessaloniki should be around the following areas:

- *Eco-friendly digital business models for startups*
- *Digital Security & cyber-crime for digital entrepreneurs*
- *Managing and understanding the quintuple helix towards fostering digital & responsible startups*

2.1 Objective

This document aims to demonstrate the good practice that our team will follow during the company's life cycle. As our project will be heavily dependant on collecting sensitive user data, digital security is a top priority good practice for us. Any business model that handles some amount of personal user data can benefit from the aforementioned good practice, and our model is not an exception.

2.2 Introduction

Our business model revolves around engaging customers by improving their shopping experience with personalized offers. Therefore leaving the private data such as indoor location, consumer habits, time spent in an establishment, etc. in an open access may, not only eliminate company's advantage before it's competitors, but also bring undesirable consequences into the clients' lives. As of now, the project is developed with the intention of using the most recent and advanced security techniques for protecting users' privacy. There is no concrete time frame for the implementation of this practice, however our company will not release the end product without the digital security practice in place.

2.3 Actors and Stakeholders

Despite the fact that digital security can not provide an impenetrable firewall between the client data and accidental information leakages, following this practice definitely brings a considerable amount of superiority before any company that does follow none. The first party who will benefit and also is the target group of this practice is the customers as even though they provide a substantial number of personal information to the business, they can be sure that it is in the owner's best interest not to let anyone else manipulate it in any way. A second benefiting party is the business owners also known as stakeholders. When is comes to the partners of this practice, many Cyber Security companies would be willing to assist in the quest of creating a protected environment for the sensitive data to be stored in.

2.4 Methodological approach

There are several steps that are necessary for implementation of this good practice. First of all, business owners should be aware of their clients' personal data importance and therefore be willing to follow the security guidelines. Secondly, all the data manipulations should be as transparent as possible, so that clients can be clearly informed about the ways in which their sensitive data is processed. Overall, the final product will not track customers' genders, therefore it respects the gender equality policy.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.5 Validation

The validation process is expected to be conducted by two main parties: business owners and customers. Business owners will be able to see the positive effect on their sales and profit margins, as well as customer loyalty, when customers will find the shopping operations to become more enjoyable and safe.

2.6 Results/outputs

This good practice is important for any company as it helps to conduct business development without being concerned about most of the problems connected with compromised user data and transparency of actions performed on the mentioned data before the local authorities. Inability to perform this practice can lead to a considerable loss in company's respect in the eyes of the public or complete termination of the company's activity in the given area of operations due to the law obligations regarding the personal data processing rules.

2.7 Impact

It is challenging to predict the overall impact of the practice on businesses over the long-term period, as no company can give a 100% guarantee to be safe against every type of malicious intent. On the other hand, even though security faults might happen from time to time, this gives the adopters of this good practice a place for improvement by showing them the weak and strong sides of the current system. The main way of doing so is by monitoring and evaluating the failed and successful breaching attempts, keeping statistics and logs. Additionally, the gathered knowledge can be shared with other similar companies in order to develop the whole sector in terms of cyber crime awareness and new means of protecting against it.

2.8 Success factors

What element distinguishes this practice from other similar ones?+
What are the conditions (institutional, economic, social and environmental) needed for the practice to be successful?+

The main element that brings difference between this practice and others is the fact that it helps business owners to take into consideration not only the very business integrity and prosperity, but also seeing their customers as something more than a bag of money – a person with their own needs, wants and rights. Clearly this practice would not be applied in our society without any external regulations that will enforce the ubiquitous usage of it. Therefore local government should support this initiative and devote resources and money on promoting and showing the advantages that come from the use of this good practice.

2.9 Constraints

The main challenge in this realm is certainly the natural resistance of human nature towards changes in the already working system. Many companies would prefer to ignore the issue until it becomes a real problem. The best way to avoid such trap is to advertise the importance of the digital security in the modern world by conducting special seminars and conferences that will additionally raise attention of the

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

already concerned people and give food for thought to ones that are still hesitant to apply the new practice to their projects. Additionally, an over-the-top protection may cause the difficulties for the company's employees to process the data efficiently. This issue should be resolved by the hired expert in the field for each given case separately as different businesses require different approaches. In order to maximize the benefits that this tool provides, every business owner should remember not to put more resources and money into protecting the element that it can possibly produce. In other words, any security scheme should not prevent the business from being economically viable.

2.10 Lessons learned

1. Every business must respect their clients' rights and privacy.
2. Digital Security's application should be limited to the purposes of the business and types of data required, as extensive protection might slow down the work.

2.11 Sustainability

	Elements needed	Cost incurred	Benefits
Technological	Modern and up-to-date technological advances as anti-viruses and software alike. Moreover, there should always be a group of available IT professionals (either hired personnel or outsource contractees).	Expenses may vary depending on many different factors such as company size, level of security requested, etc.	If executed correctly, company will be protected from the most common threats. In addition to this, IT professionals will be immediately able to counter the problems in order to prevent additional damages.
Social	Company staff should be digital security literate and be aware of the ways to recognize the potentially dangerous web-sites, emails, etc. Furthermore, it is crucial to educate personnel regarding the social engineering techniques that malicious people	Constant training programs can be cumbersome to organize both in terms of money and human resources.	Company's information will be very secure if people operating it will know how valuable it is, which in return will make it much harder for competitors or hackers to acquire it.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	may use in order to gain access to the company's information.		

2.12 Demonstration

Our final product will be handling large amounts of personal user's data, using a part of it only during the customer's presence inside the establishment and storing other for a future reference and statistics. Despite any security concerns mentioned above, the users can feel safe about their information, as it is planned to be released with the most robust security standarts currently available on the market.

2.13 Related website(s) / resources

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.