heyData

DATA PROTECTION FOR START-UPS

Competitive advantage through data protection

DATA PROTECTION FOR START-UPS

Competitive advantage through data protection

#1
Why is data protection crucial for my start-up?

#2
Why is customer trust important for competitiveness?

#3
Data protection basics

#4
What particullary start-ups need to keep in mind

#5
The use of SaaS tools

#6
How does data protection become a competitive advantage?

#7
Final tips

On the following pages we answer fundamental questions regarding data protection.

If you have any questions, please contact us via **anfragen@heydata.eu** or **+49 89 41325320**

#1
WHY IS DATA PROTECTION CRUCIAL FOR MY START-UP?

Strategic advantages through a high level of data protection

Customers expect their data to be handled correctly. Consumers are becoming increasingly aware of what misuse of their data can mean for their private and professional lives. If a start-up finds a professional solution from the beginning and thus avoids problems, data protection can become a marketing argument. On a business level, data protection makes it easier to work with partners, as well as to get investors on board. In these situations, an accurate and compliant data protection concept and correct documentation is necessary to avoid delays or negotiation breakdowns.

Data protection issues delay sales

The importance of data protection is increasing both in business and private context. The handling and protection of data is now part of the purchasing decision. For this reason, sales employees should be interested in a legally compliant data privacy solution and should be well informed to be able to answer open questions during sales meetings. Unresolved data protection issues delay the sales process by an average of four weeks (source: Cisco 2019).

GDPR compliance and penalties

Putting aside the supposedly troublesome issue of data protection for the time being can quickly take its toll on young companies. Penalties for violations affect both new and large, established companies. Furthermore, initial omissions often lead to costly adjustments having to be made later, often motivated by warning notions regarding the handling of data protection. The fines noted in the General Data Protection Regulation (GDPR) can be very high (up to 20 million euros or 4% of revenue) and jeopardize the continued existence of the company.

Does this mean that start-ups need to prepare for the worst now?
No, start-ups don't have to be generally afraid. The sanctions in the GDPR shouldn't cause fear, but rather motivate companies to see data protection as a competitive advantage. It makes sense to take greater account of data protection as a quality feature in corporate decisions. This is also because ignoring data protection can be very expensive.

#2
WHY IS CUSTOMER TRUST IMPORTANT FOR COMPETITIVENESS?

In many industries, but especially in the digital sector, the selection of suppliers and products is immense due to the internet and increasing globalization. Successfully acquiring a customer requires his or her fundamental trust, which must be created and shouldn't be violated.

> 57% of consumers would stop doing business with a company that used their personal data inappropriately. (Source: cognizant, 2016)

Therefore, data protection is not just a matter of GDPR compliance, but has an impact on reputation, customer trust and competitiveness. Especially if a breach results in a high penalty, a public impact usually follows as well. The corresponding damage to the company's image significantly reduces customer confidence. While customer satisfaction only begins after the purchase, trust already is a necessary prerequisite for a positive purchase decision.

37%
of consumers
would take legal action against a company that uses data inappropriately.

57%
of consumers
would stop doing business with a company that uses personal data inappropriately.

50%
of consumers
are willing to pay more for a company they trust.

Source: cognizant

#3
DATA PROTECTION BASICS

Digitalization makes it easier to process large volumes of data so that companies can tailor their products and services more individually to customers' wishes. This makes it more relevant to prevent data misuse and protect individuals from third parties freely using their data.

In order to strengthen the protection of private individuals, the EU-wide valid GDPR came into force. It lays down rules for handling personal data - and thus sets clear limits to companies' actions both online and offline.

Personal data

According to the GDPR, personal data is information that allows conclusions to be drawn about a natural person. They are particularly protected because their free use can have negative effects on the natural person concerned and endangers the free development of his or her personality.

Personal data are, for example, first and last name, e-mail address, address and telephone number and also the IP address of an Internet user.

Data protection on the Internet

The regulations of the GDPR must also be considered on the Internet and when designing websites. They, for example, lead to the fact that operators of websites have to ask for the consent of a site visitor before setting most cookies. Cookies are small text modules that are stored in the browser of a user and contain information. The obligation to comply with the GDPR on the Internet joins other legal obligations, e.g. to provide an imprint.

#4
WHAT PARTICULLARY START-UPS NEED TO KEEP IN MIND

Handling data in a start-up

Even if a start-up's business field isn't directly related to data, it must comply with data protection regulations. A data protection officer is very helpful for that. In the course of many activities in a start-up, questions arise that are best answered by an expert.

> The data protection consultant can answer various questions on the subject. These include the use of private laptops or mobile devices , the storage of data in a cloud or sending newsletters.

The above-mentioned activities can easily lead to data privacy violations. It therefore is important to take appropriate measures, for example by closing order processing contracts with external service providers. In order to master these challenges or at least tackle them efficiently, it's advisable to call in a data protection officer.

Does my start-up need a Data Protection Officer?

If one or more of the following criteria apply to your company, then YES:

- Your company has 20 or more employees
- You protect your office with a surveillance camera.
- Dealing with special categories of personal data is part of your business field, e.g. health data, ethnic origin, political opinions, religious beliefs or the sexual life of persons.
- Personal data is processed in order to transmit them for business purposes. This occurs in many personnel companies, e.g. recruiters or headhunters, but also applies to numerous marketing agencies.
- You regularly process data of persons under the age of 16.

#5
THE USE OF SAAS TOOLS

SaaS tools are particularly important for the work of start-ups because they are cheaper and more quickly available than traditional desktop software. The use of SaaS tools is inconceivable without processing personal data. Thus, SaaS providers and their customers are subject to data protection regulations. The GDPR distinguishes between so-called controllers and processors. Processors are external companies such as SaaS providers to whom persons in charge have outsourced tasks. Both - controllers and processors - must comply with the regulations of the GDPR and are liable for violations.

Here's what you need to consider regarding SaaS tools:

01. Only use reputable tools. If you use an external provider, you have a duty to monitor it.
02. Be careful with providers from outside the EU. You may only transfer data to them if their security is ensured by specific regulations and precautions. This is a frequently examined issue by supervisory authorities.
03. Inform your customers sufficiently about the use of the tool. This is especially necessary if the provider of the tool is located outside the EU.

#6
HOW DOES DATA PROTECTION BECOME A COMPETITIVE ADVANTAGE?

Expertise in the field of data protection

Expertise in data protection is business-critical. The manageable costs of a data protection officer usually pay off after just a few months. In particular, it can be advantageous to call in a data privacy officer when there are not yet any acute problems. A data privacy officer can prevent problems from from occurring in the first place and help to ensure that data privacy becomes part of the corporate culture. External data privacy officers are less expensive than internal ones and often have a better overall view of the industry.

Employee training

Employee training is an important element of data privacy compliance. Trained employees also minimize the risk of fines, because employees are sensitized to what data protection compliance means. Sales employees trained in data privacy can not not only score points with new sales arguments, they also have an understanding of possible reservations of your customers and can react with solutions. Furthermore, employees understand that data privacy is important and appreciate the company's commitment. Employee training also has a positive impact on the company’s culture.

Choice of server location

Choose your server location to be attractive to customers. A server location in the USA cuts you off from important business in Europe. Again, following data protection laws from the start helps position you properly on the market. Changes made later are expensive and lead to employee frustration.

IT security concept

An IT security concept helps to maintain an overview of the protective measures of a company and prevents costly data protection breaches due to system failures, the loss of know-how or data hijacking. Encryption measures or the separation of data from different customers can help to prevent data breaches altogether or, if they do occur, to reduce the risk. An overview of technical and organizational measures (TOMs) documents the status of the protective measures.

Deletion concept

A deletion concept specifies the criteria at what point in time data needs to be deleted in a company. Depending on the size and business area of the company, the creation of a deletion concept can be a time-consuming process - but one that pays off! Not only do supervisory authorities go against the storage of data for an unlimited period of time - also known as data graveyards - and impose high fines. Customers also view the indefinite storage of their data very critically. Pursuing a concept saves tedious work at a later stage, e.g. shortly before a financing round or when the supervisory authority is already “around the corner”. Nevertheless, data should not be deleted without a concept, as companies are even legally obligated to retain certain data for prescribed periods of time.

Communicate your data protection actions!

Companies like to boast that they are emission-free. Their customers see this as a sign that the company is managed responsibly. Compliance with data protection regulations also is a good way to show customers a company's sense of social responsibility. This is where you can easily stand out from your competitors!

Data privacy officer as an innovation accelerator

Data protection is sometimes seen as a brake on innovation. Wrongly so! A data protection officer takes away companies' fear of data protection. By following processes in the company from the very beginning and taking an active role in shaping them, the company is able to take data protection into account in time and even make it its strength. Data protection-compliant products and services survive better on the market than their competitors, who shortsightedly ignore the regulations.

#7
FINAL TIPS

Be proactive, not reactive and preventive, not corrective!

Do not only act when it’s too late or urgent. The best results in data protection are achieved through forward-looking planning. Therefore, don't lie back on the fact that your company is still "too small" for professional data protection consulting or that - via an outdated or unused system - you are already covered regarding data protection. heyData gives you an innovative data protection tool with the heyData platform that will really help you.

Private mobile phones and computers

Especially young companies start with limited resources and mix private and professional life even on the technical level. If you use private mobile devices, you can easily and unintentionally violate data protection regulations. Even if you don't have the resources to separate devices, you should at least define which software can and cannot be used for business purposes.

Be transparent

Only about one in five customers reads the data privacy statement (source: Data Ethics, 2016). It is therefore not suitable as a channel for making the topic of data protection interesting for customers. This is exactly why you can create additional transparency by providing customers with further, easily understandable information in advertising campaigns.

Use data sparingly!

Do not store more data than necessary. If certain data isn't important for the conclusion of a contract or the execution of a transaction, it's best not to collect it in the first place. You don't have to protect data that you don't have. Your data protection officer will be happy to help you determine what data you actually need.

Use secure passwords!

An elaborated data protection concept is a blessing, but the protection starts with small things. Insecure passwords provide easy access to your systems for third parties. Make sure that passwords have at least 8 characters, contain special characters and do not contain names or familiar terms.

heyData

Do you have questions regarding this topic or about data protection?

Our experts will be happy to check your company through a non-obligatory consultation to identify data protection gaps.

Your contact persons from heyData from left to right:

Miloš Djurdjević
Co-Founder & MD
milos@heydata.eu

Daniel Deutsch
Co-Founder & MD
daniel@heydata.eu

Martin Bastius
Co-Founder & CLO
martin@heydata.eu