Brandheroes™
GDPR ANALYSE 2018

Authors

Thomas Bro Hansen, CEO
Mette Frich, GDPR Consultant
Josephine Ejlersen, Legal Consultant

Date

23 May 2018

CONTENT

4.0 TECHNICAL SECURITY MEASURES

4.1 User Access Management

4.2 Privacy by Design

4.3 Maintenance and service

4.4: Data encryption

4.5 Anti-virus

4.6 Data portability

5.0 IMPACT ANALYSIS

I confirm that the content of this report is true and account for the technical and organizational conditions according to all aspects of personal data handling and storage within Brandheroes ApS.

Thomas Bro Hansen
CEO / Co-founder

Appendix 1:	Terms & Conditions (Influencers)
Appendix 2:	Terms of Purchase (Customers)
Appendix 3:	Data Processing Agreement Vendor (Brandheroes act as data controller)
Appendix 4:	Data Processing Agreement Customer (Brandheroes act as data processor)
Appendix 5:	Standard employment contract
Appendix 6:	External data policy (Hero handbook)
Appendix 7:	Internal data policy (Hero handbook)

1.0: INTRODUCTION

Brandheroes is a Danish based digital company specialized in influencer marketing. Brandheroes' platform connects local micro-influencers (regular people that are carefully casted and selected rather than celebrities) with lifestyle brands for authentic collaborations, and enables them to become Brandheroes by sharing the love for the brands on social media.

The purpose of this report is to clarify that and how Brandheroes lives up to the standards outlined in GDPR and the Danish Data Protection Act. To that end, the report documents and gives and overview of the relevant data streams and processes.

In terms of methodology, the report draws on workshops with Brandheroes' management, HR, development and Legal, where all relevant activities have been analyzed and discussed.

2.0 GENERAL OBSERVATIONS

The purpose of this section is to provide a systematic overview of the data requirements, classifications and processes that apply to Brandheroes' business.

2.1 Categorisation of data subjects

Brandheroes has identified five different categories of data subjects:

Influencers

Influencers are ordinary users of Social Media (Instagram), whom Brandheroes reach out to with the purpose of promoting products and services from Brandheroes' customers (brands).

Employees

Brandheroes' current and former employees and applicants to vacant positions.

B2B-customers

Members of staff with Brandheroes' customers are considered as potential data subjects due to the possibility of Brandheroes receiving personal data, e.g. through e-mails. Furthermore, Brandheroes gather and store information about B2B-customers and business contacts in a CRM system.

Vendors and suppliers

Vendors and suppliers are defined as freelance agents or enterprises from whom Brandheroes source products and services. Given the continuous nature of Brandheroes' dialogue with such vendors and suppliers, Brandheroes is likely to come into possession of data regarding these. Furthermore, Brandheroes' collaboration with some of the vendors and suppliers are governed through formal data processing agreements.

Potential customers and partners

Physical persons as well as enterprises with a potential interest in Brandheroes but no current business relations.

2.2 Legal framework for the processing of personal data

It is a key implication of GDPR that the processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Purpose of collecting and recording personal data: Personal data are a requirement in order to identify and contact relevant profiles among Social Media users (primarily Instagram users) with the purpose of engaging these users as influencers for Brandheroes' customers.
In general, Brandheroes' processing of personal is based on consent from the data subjects concerned as well as on legitimate legal interest. For instance, influencers give their consent via the Terms & Conditions, and employees via their employment contracts in combination with the staff manual (Hero Handbook)

The general and primary purpose of collecting and processing employees' personal data is administrative. The primary data source is employees themselves, e.g. from application, performance reviews etc. Personal data used for HR purposes are processed in compliance with the regulations set out by the Danish Data Protection Agency. No specific consent is required to process such data – as long as processing is relevant as serves a relevant legal interest.

2.3 Classification of data

Under the framework of GDPR, Brandheroes has classified personal data as either:

- Generic,
- Semi-sensitive, or
- Sensitive.

From its very outset, Brandheroes has sought to limit the collection of semi-sensitive and sensitive personal data to an absolute minimum. That is, the company has a policy of only recording sensitive personal data about employees where such recording is strictly necessary for administrative purposes, e.g. in case of long-term absence due to illness. Furthermore, employees are the only of the abovementioned categories of data subjects that are registered with personal identification numbers (CPR). For further information about security and privacy measures regarding sensitive personal data, please refer to Section 3.8.

Brandheroes is aware of the risk of inadvertently coming into possession of sensitive personal data regarding other categories of data subjects through e-mails and other means of communication. Work is being done to secure a relevant level awareness among employees, and in general employees are asked to delete all irrelevant data and securely process all relevant data (Appendix 6).

2.4 Special measures regarding data subjects below the age of 16

Brandheroes is aware of GDPR's emphasis on especially protecting data subjects below the age of 16 and the imperative to gather parents' consent. Until now, Brandheroes has not collected and recorded personal data from young data subjects, but in case such collection should become relevant in the future, measures will be taken to ensure proper consent management.

2.5 Data sourcing

Data about potential influencers is primarily assembled from social media such as Facebook and Instagram. The nature of data is mainly publicly available information such as profile name and URL. In addition to this, Brandheroes communicate with potential and current influencers, as well as other data subjects, via digital channels such as e-mail and Messenger.

2.6 Business activities outside the EU

Given that a number of Brandheroes' customers are active in other jurisdictions than the EU, other regulatory regimes than the GDPR can at times apply to Brandheroes' activities. It is Brandheroes' general policy, when the company is conducting its business outside the EU that the rules in GDPR shall always serve as a minimum standard on top of which specific rules of the jurisdiction in question can be added.

When entering into collaboration agreements with customers operating outside the EU, it is Brandheroes' policy to always base the collaboration on specific terms-of-purchase. Regarding its activities within the EU, Brandheroes shall answer to the competent authority, namely the Danish Data Protection Agency.

Given that Brandheroes is registered and has its headquarters in Denmark, and all material decisions regarding data processing and privacy are made here, the company considers its structure to be relatively uncomplicated. All else equal, this should be conducive to the company's ability to comply to relevant regulation.

2.7 General mapping of personal data

In order to secure a sustainable structure in the company's data processing and storage, Brandheroes has created the following general mapping:

Category	Data location	Remarks
Influencers	Brandheroes' own platform and app Databases (MongDB) Hosting (Digital Ocean) Mails (Gsuite, Unoeuro) Webshop (Shopify) Brandcoins app (Smile.io) Shipping app (Weshipper) Social Media Direct Messenger Newsletter (Mailchimp) Auto Emails (Mandrill) File and Data storage (DropBox)	
Employees (and applicants)	File and Data storage (DropBox) Mails (Gsuite, Unoeuro) Payroll services (Dataløn) Pension services (Scandia) Accountant BDO Public Authorities	Due to the utilization of data such a CPR-numbers and the potentially sensitive nature of data processed, increased security standards apply to this category (see Section 3.8). Only management and HR have access to data about employees. As a rule, data is stored for the duration of the employment plus five years. Applications from candidates that are not hired are kept for six months.
B2B-customers	CRM (HubSpot) Mails (Gsuite, Unoeuro) ERP (Dinero) Newsletter (Mailchimp) File and Data storage (DropBox)	
Vendors and suppliers	File and Data storage (DropBox) Mails (Gsuite, Unoeuro) Project management (Trello, Bitbucket) IT Minds Cubas	

Potential customers and influencers (Marketing)	CRM (HubSpot) Mails (Gsuite, Unoeuro,) Newsletter (Mailchimp) File and Data storage (DropBox) Website (Wordpress) Landingpages (Kickoff labs)	

Brandheroes strive to be a completely paper-free office, which means that all physical documents are scanned and stored in the Dropbox application before paper copies are securely shredded. If, at a later stage, the legal or other requirement to store physical documents should arise, processes will be revisited.

3.0 ORGANIZATIONAL DATA PRIVACY MEASURES

The purpose of this section is to provide an overview of the governance, organizational structures, policies and procedures that are put in place to secure Brandheroes' compliance to GDPR.

3.1 Controller

Brandheroes has assessed that the company is not obliged by GDPR to appoint a Data Protection Officer. This general assessment is based on the fact that Brandheroes is a small privately owned company that does not process significant amounts of sensitive personal data.

As controller, Brandheroes has appointed Thomas Bro Hansen, who as CEO is part of the day-to-day operational management as well as the Board of Directors. The main purpose of anchoring the data responsibility with top management is to secure strong centralized monitoring and control of data privacy.

The main role of the controller is to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. Those measures shall be reviewed and updated when necessary.

3.2 Instructions to employees

Given that most of Brandheroes' employees process (mostly non-sensitive) personal data in one way or another, it is necessary to ensure an appropriate level of organizational knowledge of the key aspects of GDPR and other relevant regulation.

That is, all members of staff need to be aware of:

- The lawfulness and relevance of data processing as well as the identifiable purpose behind the processing of personal data
- The correct and proportional utilization of this data
- The aim to minimize the processing of personal data to what is necessary in relation to the defined and lawful purpose, and to delete all data, when it is no longer relevant
- Recording personal data in compliance with company guidelines
- The difference between ordinary (non-sensitive) personal data and sensitive personal data, so that the recording of unnecessary personal data about external data subjects is avoided
- The necessity of receiving relevant consent from external stakeholders
- General data hygiene, i.e. compliance to company guidelines about processing and storage.

To make employees aware of the applicable principles and guidelines, a section of the staff handbook ("Hero Handbook") is dedicated to personal data processing. The section is named "External data policy" (Appendix 6) and shall be viewed in connection with the obligations set out in each staff member's employment contract (Appendix 5):

"The employee is under a duty to adhere to ordinary guidelines for the employees in the company as well as special rules regarding the performance of the work. An employee handbook (hero handbook) containing all material guidelines applicable to the employees in the company exists in physical form, which will be handed out at the employment. The employee is required to keep him-/herself updated regarding changes in the employee handbook via the company DropBox."

In addition to this, all employees have accepted confidentiality regarding "matters that may be termed business secrets including all data information regarding influencers and customers related to the company":

"The employee is bound by a general confidentiality agreement during employment as well as after termination, with regard to matters that may be termed business secrets including all data information regarding influencers and customers related to the company. Thus, the employee is not entitled to convey information to third parties who are not generally known in the industry. Reference is made to sections 1 and 19 of the marketing act. Breach of confidentiality is a gross breach and may lead to employment consequences."

Staff members responsible for coordinating influencer campaigns and hence engaged with the concrete processing of personal data, are contractually obliged to and thoroughly instructed in assessing each individual campaign in relation to data necessity and relevance.

When at least one of the following conditions apply, campaigns are approved by the data controller:

- Non-EU countries involved
- Utilization of background variables such as influencers' clothing size etc.

Finally, all employees are instructed to pay close attention and diligence to the correct recording of data. Wherever possible, data is cross-checked, e.g. addresses which are cross-checked via Google. When onboarding new influencers, special attention is paid to the correct registration of core data.

3.3 Disclosure and transparency

Brandheroes has implemented two main pieces of documentation targeted at data subjects (influencers and employees) that are meant to ensure transparency about the processing of personal data as well as data subjects' general rights:

- Terms & Conditions – influencers (Appendix 1)
- Staff manual – Internal data policy (Appendix 7)

Potential influencers are contacted by Brandheroes via Social medias public comments and direct messages features. When accepting to become influencers for Brandheroes, they agree to the abovementioned Terms & Conditions, thereby giving Brandheroes legal consent.
Accept is given by the influencer checking of a non prefilled terms and conditions checkbox and submits it to Brandheroes platform together with all other relevant signup data, for Brandheroes to deliver their service to the influencer.

In the document Terms & Conditions, which is drafted in a clear and uncomplicated language, influencers are informed about the data processing carried out by Brandheroes as well as about Brandheroes' identify, the purpose and legal basis of data processing, storage period and the right to complaint to the supervisory authority (Danish Data Protection Agency). Finally, data subjects are informed that data can potentially be processed outside of the EU.

Moreover, data subjects are informed about their rights, e.g. the right of access, the right of rectification, the right to erasure, the right to restriction of processing and the right to data portability.

To inform employees about their rights as data subjects, Brandheroes has issued an internal data policy which forms part of the staff manual ("Hero Handbook"). As mentioned above, employment contracts, state the obligation for employees to make themselves familiar with the information included in the Hero Handbook. That is, by signing contracts employees give Brandheroes their legal consent to data processing. Similar to other legal documents, employment contracts are digitized and stored in Brandheroes records to which only HR and top management have access.

3.4 Procedures for erasing data

Brandheroes has identified four situations which call for the systematic erasure of personal data:

- When data subjects (influencers, employees) or enterprise (B2B-customer, business partner) actively call upon their right to erasure
- When data turns out to be faulty and therefore demand rectification
- When data is no longer relevant
- When data has been reported as inappropriate (Brandheroes' app contains a feature by which users can report both content and comments as inappropriate)

In all of the above cases, Brandheroes' general data mapping (see Section 2.7) serves as a good point of reference for localization and erasure of data. That is, the data mapping gives an overview of where the different types of personal data concerning the different categories of data subjects are stored, and thereby gives management a strong foundation for the manual process of identifying and erasing the data in question.

Furthermore, in the staff manual (Appendix 6) employees are instructed to continuously assess their records e-mails and Messenger content in order to secure the timely erasure of irrelevant content. Finally, management goes through an annual compliance process (see below) in which all personal data is assessed with the purpose of identifying data that is no longer relevant.

3.5 Annual compliance process

Each year in December, a compliance process is carried out with the purpose of ensuring compliance to GDPR and other relevant regulation. As a part of this process, data privacy and security measures are assessed and potential breaches are recorded and if relevant reported.

As part of the compliance process, the following documentation is assessed:

- General mapping of personal data (is data still processed and stored in the specified locations)
- Terms & Conditions (framework for engaging with influencers)
- Terms of Purchase
- Data processing agreements where Brandheroes act as data processer for partners
- Data processing agreements where partners process Brandheroes' data
- Staff manual ("Hero Handbook") – external data policy
- Staff manual ("Hero Handbook") – internal data policy

The outcome of the process is a report targeted at the relevant external stakeholders, e.g. partner for whom Brandheroes act as data processer. The report is published on Brandheroes.com.

3.6 Procedure for reporting data breaches

In the event of leakages or other breaches of data privacy, Brandheroes has established a procedure to ensure that the competent supervisory authorities (Danish Data Privacy Agency) and the data subjects concerned are informed. The responsibility for this procedure lies with the controller.

In the event of a breach, Brandheroes will notify the relevant stakeholders about:

- The character of the breach (categories, number of data subjects affected etc.)
- Consequences of the breach
- Mitigating actions carried out by the controller
- Relevant contact information
- Records of procedures and measures in place in the period when the breach occured

3.7 Data processing agreements

In order to make sure that external partners (data processors) comply with GDPR and other relevant regulation, all data processors enter into a data processing agreement with Brandheroes (Appendix 3). When entering into partnerships with data processors that have already drafted their own GDPR compliant data processing agreements, these agreements can be used as an alternative to the template shown in Appendix 3. Similarly, Brandheroes is obliged to comply with the same regulation when acting as a data processor for other parties. Refer to Appendix 4 for Brandheroes' framework data processing agreement.

3.8 Special guidelines regarding employee data

Brandheroes' data stream analysis has generally disclosed that the only category of data subjects, from whom Brandheroes come into passion of non-negligible quantities of sensitive personal data, is employees. Therefore, special guidelines are in place to ensure that due diligence and caution is shown in this specific area:

- Access to staff records is limited to the few people who have relevant purpose and need for processing the data (top management and HR). Only this group can access the specific area of Brandheroes' digital storage system, where employee data is kept, and only this group have access to the information given to external entities such as BDO (accountant), Dataløn (payroll services), Scandia (pension services) and public authorities. Members of staff charged with handling employee data are specifically instructed in the proper processing of such data.

- When sensitive personal data is transferred via e-mail, Brandheroes comply to the Danish Protection Agency's recommendations about encryption.

- As a general rule, USB-keys and other external storage devices are not used in Brandheroes. In the event that members of staff come into possession of such devices containing sensitive data, these must be stored in a locked cabinet.

Furthermore, it is worth noting that Brandheroes source services in the HR area from professional vendors of pay services, pension services, health services etc. All else equal, these vendors are expected to comply to high standards in data privacy. In general, vendors' IT-systems are designed to log and register users' behaviour, e.g. block unauthorized access to systems. These partners are considered as data processer, ref. Section 3.7.

Finally, Brandheroes is aware that the utilization of staff photos on the company website requires specific and revocable consent from of the staff members in question.

4.0 TECHNICAL SECURITY MEASURES

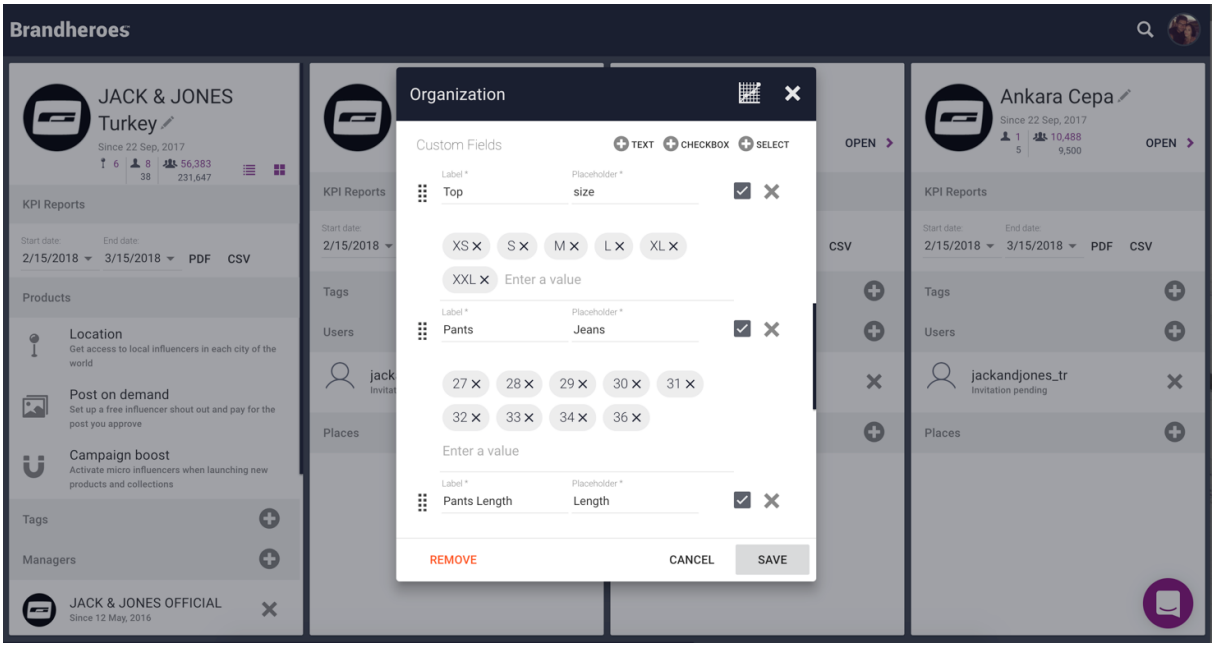
As a part of the data stream analysis, Brandheroes has carried out an assessment of the technical utilities and procedures used to ensure maximum data privacy. This assessment has also served to ensure that the demands and standards set out in GDPR is reflected in future development of IT-systems etc. This purpose in also addressed in the data processing agreements (see Appendix 3 and 4) used to govern relations with external partners.

4.1 User Access Management

As a general principle, systems, e.g. data storage systems, are designed and set-up so that they can only be accessed by persons with a relevant need and purpose for such access. Hence, general user access management and access codes are used to restrict access to PCs and other electronic equipment containing personal data. Only persons with relevant need and purpose, can obtain a code. Access codes are personal and may not be transferred to other or left visible to others. Codes and authorizations are checked at least every six months.

4.2 Privacy by Design

Brandheroes' digital platform is designed to accommodate the principle of Privacy by Design. That is, the platform is designed with the aim of minimising the processing of personal data so that only personal data which are necessary for each specific purpose of the processing are processed. Specifically, Brandheroes' back-end is designed with so-called custom fields which means that the members of staff handling each campaign are only prompted to enter into the systems the data that are relevant for the actual case.



4.3 Maintenance and service

When performing maintenance and service of data equipment containing personal data, and when selling or scrapping such equipment that is no longer in use, Brandheroes pays great attention to taking the proper security measures. Concretely, this means that all personal data is deleted or transferred to other media before equipment is handed over to third parties.

4.4: Data encryption

Data encryption is used, whenever Brandheroes transfer data.

4.5 Anti-virus

Firewall and virus protection are installed on all company computers with access to the internet and other digital networks.

4.6 Data portability

In general, Brandheroes' data processing structure and IT-systems are well-equipped to accommodate the principles of data portability set out by GDPR. That is, systems are designed to accommodate the of the data subject's right to receive the personal data concerning him or her in a structured, commonly used and machine-readable format.

5.0 IMPACT ANALYSIS

Given that Brandheroes does not process large amounts of sensitive personal data, the company is not obliged to perform a formal impact analysis. However, to sum up the findings of the data stream analysis above, we have chosen to include a brief overview of the expected likelihood and consequences persisting the different types of data and different categories of data subjects handled by Brandheroes.

Impact					
Very high					
High		2			
Low		1, 3, 4, 5			
Very low					
	Very unlikely	Unlikely	Likely	Very likely	**Probability**

1 = Influencers
2 = Employees
3 = B2B-Customers
4 = Vendors & Suppliers
5 = Potential Customers and Partners