PRIVACY POLICY
(Latest version: 30 September 2023)

1. INTRODUCTION

This privacy policy describes how personal data is processed by ON Social. For any data protection queries contact us using form on the website.

This Privacy Policy should be read in conjunction with our Terms of Service and describes the way that we deal with the data of customers of our Services and Influencers (both terms as defined in our Terms of Service).

2. WHAT PERSONAL DATA IS PROCESSED AND THE LEGAL BASIS FOR PROCESSING

2.1. Customers

There are different types of information we obtain, whether directly from you at sign up or automatically via your device when you use our Services. Examples of information provided and legal basis for processing is set out below.

Information you provide Us with:	**Legal basis for processing and reason for collection**
1. Full name, company address, company name	Performance of the contract with you. We require to identify you for the contractual relationship between the parties.
2. Email and social network profile	Performance of contract with you and our legitimate interests, if related to marketing. We require your email and/or social network information to log you into the system and to provide you with the Service, reports, Service related updates, communications and other important information. If we do use your email to contact you for marketing purposes, it will be in Our legitimate interests to do so, but you will always have a chance to opt out of such marketing communications for similar products and/or services prior to first (and any subsequent) communication. You may opt out at any time.

The rest is the technical information that must be processed in order to provide you with our services (i.e. Internet Protocol (IP) address).

2.2. Influencers

On behalf of our Customers (data controllers), we, as data processors, obtain relevant data from publicly available sources (websites, social networks and similar). We only process information based on our customers' request. Such information that you, an Influencer, will have already shared with the world.

Upon receipt of a request from a customer of our Service, we identify relevant Influencers and allow the parties to get in touch with each other for a mutually beneficial partnership.

For instance, you may have listed your email and/or telephone number in your profile on a social network. You promote a healthy lifestyle and do not mind earning income from such an activity, looking for an opportunity to collaborate with a business.

Our potential customer is a health food store. The customer approaches us in order to find a relevant Influencer to promote its business. We would then try and identify you (rather than someone interested in unhealthy eating) as the right person for the business. You will get a chance to earn income doing what you love and our customer will save time looking for the right person to promote its business.

Our customers, as data controllers, undertake to have a legal basis for processing Influencer personal data before retaining us to provide Services to them. They will have contacted you upon first collection of personal data or at the time of first contact with you.

Example of data processed on behalf of our customers, the data controllers:

Information Influencer provides publicly:	**Legal basis for processing and reason for processing**
1. A link to Influencer profile, full name. avatar, language, biography, gender, country/city/state, brand and common interests, notable engaged users, sponsored posts. 2. Email and social network profile or a telephone number. 3. Images, graphics, photos, audio and video clips, links to external websites and other content or materials. 4. Any other relevant content, available to public in general (audience data and other statistics).	Influencers publish their personal data openly on the Internet for various reasons. Where we identify a reason for the Influencer to publish its data publicly as that of looking for a business opportunity, we find that it is in the **legitimate interests** of third parties to process such personal data for commercial purposes without affecting Influencer's fundamental rights and freedoms and in line with data protection legislation. The reason for processing: to allow our customers to choose an Influencer for their business purposes and assess the effectiveness of each Influencer's potential reach and benefit.

2.3. Contact Form Queries

Where you contact us via a form on the website or email us with a query, we only use the details provided (such as your email address, name and content of your message) in order to respond to the query. We do not use such data for any marketing or similar activity.

3. WHAT WE DO WITH PERSONAL DATA

3.1. Customers

We use Customer contact details and payment information to establish, support and conduct customer relationships as necessary for the performance of Services. Should the Customer fail to provide the personal data we need, we may be unable to complete the transaction. We only contact Customers with service related information. Where marketing is involved, Customers have an option to opt out at any time before first (and any subsequent) contact.

3.2. Influencers

As part of our Service to our customers, we may enrich the data about Influencers with additional information through our unique algorithm, in order to provide a more complete picture of the Influencer for the business. However, as we only provide a statistical service on behalf of our customers, as a data processor, we do not and cannot dictate the purposes, the data controllers, for which the data is further used by those data controllers. However, we do have

contractual warranties whereby data controllers undertake to only use the data for legal purposes and in full compliance with the relevant data protection laws.

4. HOW LONG PERSONAL DATA IS STORED FOR

4.1. Customers

We store your data while our agreement with you is in force and thereafter for the legally required duration to confirm the transaction and any dealing with you.

4.2. Influencers

As stated above, we process information that on behalf of our customers – data controllers. We store Influencer data while our agreement with the customers is in force and effect or until an instruction from our customers to delete particular data.

Where we receive a request from an Influencer with regards to the deletion of the data, we pass that message on to the relevant customers and effect the deletion and/or provision of relevant information within the timelines under relevant law.

5. SECURITY MEASURES USED BY US

Although, no data is ever safe, all personal data is kept with our third-party processors on secure servers, who are in full compliance with international information security requirements. We use the recommended industry practices to keep access to such data secure (mixture of common sense and best practices).

We use appropriate level of technical and organizational measures to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed. Those include the following:

(1) Protective measures for physical access control:
We secure access to the premises via ID readers, so that only authorised persons have access. The ID cards can be blocked individually; access is also logged. Furthermore, an alarm system is installed in the premises, preventing infiltration by unauthorised persons. The alarm system is linked to a locking mechanism for the doors.
(2) Protective measures for system access control:
Each employee has access to the systems/services only via his/her own employee access. The access rights involved are limited to the responsibilities of the respective employee and/or team. We regulate access to our own systems via password procedures and the use of SSH keys of at least 1024 bits in length. The SSH keys strengthen the productive systems against attacks that target weak passwords, as the password-based access to the relevant systems is disabled. We have, in addition, a regulation for the creation of passwords. This guarantees higher security also for systems that offer password-based access. Passwords must meet the following requirements: At least 8 characters long At least 1 letter in upper-case At least 1 letter in lower-case At least 1 number At least 1 non-alphanumeric character

Our systems are protected by firewalls that reject all incoming connections by default. Only connection types defined by exception are accepted.

(3) Protective measures for data access control:

All servers and services are subject to continuous monitoring. This includes the logging of personal access in the user interface.

Due to the close proximity of the employees, a visual inspection is possible at any time.

Locking and/or logging off when leaving work is prescribed in writing and is practised.

(4) Protective measures for transfer control:

The handling of local data storage devices, e.g. USB sticks, is regulated via agreements.

Access to the systems from outside the company network is possible only via secure VPN access.

(5) Protective measures for input control:

Our employees do not work directly at database level, but instead use applications to access the data.

IT employees access the system via individual access and use a common login, as there are very few employees and these sit in close proximity of each other and monitor each other by agreements and visual inspections.

(6) Protective measures for availability control:

We ensure the availability of data in several ways. On the one hand, there is regular backup of the entire system. This steps in if the other availability measures fail.

Critical services are operated redundantly in multiple data centres and controlled by a high-availability system.

Our workstations are also protected with the usual measures. For example, virus scanners are installed, laptops are encrypted.

(7) Protective measures for separation control:

To separate data, We use logically separate databases so that no accidental reading of data by unauthorised persons can occur.

Access to the data itself is also restricted by the fact that employees use services (applications) which control access.

6. YOUR RIGHTS

You have a wide array of rights that we respect. Among those, the right to:

- Require access to your personal data;
- Require rectification of your personal data;

- Require erasure of your personal data;
- Withdraw consent to processing of your personal data, where applicable;
- Lodge a complaint with your national supervisory authority (if you are based in the EEA) if you believe that your privacy rights have been breached.

We act as a data processor only and act upon instructions of our customers (the data controllers). Therefore, in order to exercise your rights, you should contact the data controllers directly. However, if you believe that the data controller is not responding to your query or is in breach of its data protection obligations, feel free to contact us directly and we will pass the message on to our customers to ensure your rights are protected.

7. COOKIES AND SIMILAR TECHNOLOGIES

We use strictly necessary cookies to operate the website. However, should any other types of cookies be used (such as aggregated, non-identifying, electronic data collected from use of our Sites and Services to operate, analyze, improve, and develop our Sites and Services) you will be given a choice to decline such cookies.

8. CHILDREN'S PRIVACY

We never knowingly collect or solicit any information from anyone of 13 years and younger nor provide services that may relate to the same. If parents or guardians believe that We hold information about their children aged 13 and under may contact Us.

9. NOTICE FOR CALIFORNIA RESIDENTS (CCPA AND CALOPPA)

For the purposes of paragraph (v), section 1798.140 California Consumer Privacy Act of 2018 (the CCPA), we are a Service Provider and, as such, any queries relating to the processing of Personal Information (as defined in the CCPA) shall be sent directly to a business (as defined by the CCPA). However, general information required by the CCPA is listed below:

- in accordance with subparagraph (A) the list of consumer rights is specified in section 6 above;
- in accordance with subparagraph (B) the categories of personal information We collect and have collected about consumers in the preceding 12 months are listed in section 2 above;
- There is no consensus on how mobile application companies should interpret the DNT signals. For the purposes of the CalOPPA, We do not currently respond to DNT signals whether that signal has been received on a computer or a mobile device.