Staffers Privacy Policy

Staffers as a company offer a software as a service (**“Platform”**) where it is possible to search and request, work on jobs as a staffer and as a company present your company profile, add jobs and add staffers to jobs.

We are committed to your privacy

We appreciate that you put your trust in us when you provide us with your information and we do not take this lightly. Your privacy is our top priority. The personal data will be stored only as long as it is necessary for providing our services.

We understand that online services can be confusing and hard to understand on how they manage your data. That is why we try to write our policies in plain language and avoid complicated language so that you can easier understand how we work.

Responsibility

We are a SAAS platform (Software as a service) that help users and companies connect with jobs. Companies can create jobs and staffers can search and apply for them. A contract is set up for each company's job and staffer that is accepted for it. Thereafter they can chat and communicate about the job , and the platform gives the tools needed for the parties to lower cost and communication, making the job get done more efficiently.

For a better overview of the personal data and the different roles, please see **Appendix A** to this Privacy Policy.

What information is processed?

In **Appendix A** to the Privacy Policy, we describe what kind of personal data and other information that is processed in connection with our Platform, and what information is public.
«**Personal data**» means any information relating to an identified or identifiable natural person (the «**Data Subject**»).

Contracts are secret and not public to any other parties than the parties writing the contract.

Analytics

While the Actors are interacting between each other, the Platform itself is logging these actions to create actionable analytics for the Actors. No personal info or direct analytics of a Company or User or Jobs is shown to any party, rather a sample of the data and grouped information to get a better overview of what is happening in the system.

- For us, as the architects behind the Platform, this is necessary to understand how Users act - and helps us to build a better Platform and service.
- Companies can get statistics on usage such as the amount of views of a job and what hours they get responses, no personal data is used here.
- Users can learn from analytics how to better perform at their jobs and be a more competitive worker to get more and better jobs.

Recipients of personal data

The recipients or categories of recipients of the personal data are listed in **Appendix A** to this Privacy Policy. **Appendix A** also includes information about whether the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. Please contact us in accordance with the last section of the Privacy Policy for such information.

Privacy settings

It is important to us that your data privacy is protected. We don't sell your data. We have built our Platform so it analyses your interactions with Users and companies on the site to better find relevant Content that fits you and thus making the user experience better. If you don't want us to store your interactions this can be turned off in your privacy settings. This however will terminate your account as we cannot deliver this service without tracking interactions.

Access to user Data

We limit our personnel's access to Customer Data as follows:

- Requires unique user access authorization through secure logins and passwords, including multi - factor authentication for Cloud Hosting administrator access and individually assigned Secure Socket Shell (SSH) keys for external engineer access;
- Limits the Customer Data available to our personnel on a "need to know" basis;
- Restricts access to production environment by our personnel on the basis of business need
- Encrypts user security credentials for production access
- Data encryption
- Data Management
- Network Security, Physical Security and Environmental Controls
- Independent Security Assessments
- Incident Response

Rights of the Data Subjects

Right of access

You have the right to receive confirmation as to whether your personal data is being processed by us, as well as various other information relating to our use of your personal data and copies of that information. You also have the right to request access to your data which we are processing.

Right to erasure and rectification

You have the right to request us to erase your data. We shall comply with your request without delay unless an exception to compliance applies, for example if the data is required to establish, exercise or defend legal claims. You also have the right to make us correct any inaccurate personal data about you.

Right to object

You have the right to object to us processing your data. If you ask us to stop processing your data, we will stop processing your data unless we can demonstrate compelling grounds as to why the processing should continue in accordance with data protection laws or, if the information is required to establish, exercise or defend legal claims.

Right to restriction

You have the right to request us to erase your data. We shall comply with your request without delay unless an exception to compliance applies, for example if the data is required to establish, exercise or defend legal claims. You also have the right to make us correct any inaccurate personal data about you.

Right to withdraw Consent

You have the right to withdraw your consent at any time. To do this, you should contact us in accordance with the last section in this Privacy Policy.

Right to data portability

You have the right request that you receive copies of the relevant data provided by you in structured, standard machine-readable format and, where technically feasible, to request that this information is transmitted directly to another controller.

Legal basis

The legal basis for our processing relating to the purpose of providing our services, are:

1. For giving you access, registering in and use of the Platform. This processing is necessary for the purposes of the legitimate interests

pursued by us and our Customers, cf. the General Data Protection Regulation art. 6(1)f. The legitimate interests are providing the Platform for business and private purposes and contributing to innovation and information sharing. These interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

2. Analytics. The processing is necessary for the purpose of the legitimate interests pursued by us, cf. the General Data Protection Regulation art. 6(1)f. We are using the information for improving our services, making better decisions and providing support.
3. For marketing purposes. The data subject has given consent to the processing of his or her personal data for this purposes, cf. the General Data Protection Regulation art. 6(1)a.

Contact us

If you have any questions regarding the Terms & Policies, data processing or to exercise your rights, please contact us at support@staffersapp.com

If you believe that your data protection rights have been breached by us, please let us know. You also have the right to lodge a complaint with Datatilsynet, the supervisory authority for data protection issues in Norway: https://www.datatilsynet.no. We appreciate the chance to deal with your concerns before you approach the supervisory authority, so please contact us in the first instance.

Data Processing Agreement

Introduction

This Agreement sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller.

This Agreement has been designed to ensure the Parties' compliance with Article 28, sub-section 3 of **Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC** (**"GDPR"**), which sets out specific requirements for the content of data processing agreements.

Description of the processing being contracted out

The data controller offers software and services based on solutions developed and provided by the Data Controller (**Staffers Platform**). The platform gives the possibility for users to search for jobs and create jobs as well as chat to each other and sign contracts between each other.

The Data Controller and controller is authorized to process data on behalf of the users, the necessary personal data for managing the platform . The personal data processed are mentioned in **Appendix A** to the Agreement. Accordingly, the subject-matter is collecting, storing, sharing, transferring and deleting personal data in connection with the users creation, administration and use of the staffers jobs and companies. This also includes the administration of users and contracts connected to the jobs and companies.

The purpose of the processing is to provide an online electronic system that helps users and companies to create and search for jobs, as well as providing contracts between the two parties. The nature of processing is storing , processing and transferring data between the two parties in relation to the administration of users and connection between staffers, jobs and companies. The platform admins cannot see the personal data sent between the parties it is automated to help the users and workflow be more efficient.

This Agreement shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR or other legislation.

The rights and obligations of the Data Controller and Data processor

The Data Controller shall be responsible to the outside world (including the data subject) for ensuring that the processing of personal data takes place within the framework of the GDPR.

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. Those measures shall be reviewed and updated where necessary.

The Data Controller shall therefore have both the right and obligation to make decisions about the purposes and means of the processing of personal data.

The Data Controller shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised in law.

Confidentiality

The Data Controller shall ensure that only those persons who are currently authorised to do so are able to access the personal data being processed. Access to the data shall therefore without delay be denied if such authorisation is removed or expires.

Only persons who require access to the personal data in order to fulfil the obligations of the Data Controller shall be provided with authorisation.

Security of processing

The Data Controller shall take all the measures required pursuant to Article 32 of the GDPR, which stipulates that with consideration for the current level, implementation costs and the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The above obligation means that the Data Controller shall perform a risk assessment and thereafter implement measures to counter the identified risk. Depending on their relevance, the measures may include the following:

1. Pseudonymisation and encryption of personal data
2. The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Use of Sub-Processors

The Data Processor shall meet the requirements specified in Article 28, sub-section 2 and 4, of the GDPR in order to engage another processor (Sub-Processor).

The Data Processor shall therefore not engage another processor (Sub-Processor) for the fulfilment of this Agreement without the prior specific or general written consent of the Data Controller.

Appendix B of the Agreement contains the Data Controller's terms and conditions that apply to the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Data Controller.

Transfer of data to third countries or international organisation

User and companies shall be permitted to process their own personal data on documented instructions from the Data Controller, including as regards transfer (assignment, disclosure and internal use) of personal data to third countries or international organisations, unless processing is required under EU or User State law to which the Data Processor is subject; in such a case, the

Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. GDPR Article 28, sub-section 3, para a.

Notification of personal data breach

On discovery of personal data breach at the Data Controllers facilities or a sub-processor's facilities, the Data Processor shall without undue delay notify the Users.

Erasure and return of data

On termination of the processing services, the Data Controller shall be under obligation, at the Data Controller's discretion, to erase or return all the personal data to the Users and to erase existing copies unless EU law or Users State law requires storage of the personal data.

Inspection and audit

The Data Controller will regularly each year inspect routines and make sure users have

Data Controller and Data Processor contacts/contact points

Appendix A. GDPR - Data Table

	Type of data?	What data?	Why?	Where data is saved
	Staffers profile information	firstname, last name, profile image, gender* birthday* description, mobile number, Experience (Company, Job title, reference, Start and End date), Postal code* , Street address* City, Country Languages, Salut certificate number*, BankID*, Age, app version	Staffers need to fill in this information in order to apply for a job, so business can see if he is eligible and qualified.	Firestore and Super admin *Is only for Firestore
	Browsing jobs	GPS Location, Address	We save this data on order to display relevant search results when browsing jobs	Firestore and Super admin
	User activity overview	Jobs completed, Jobs upcoming, Jobs pending, Total jobs, Total payout, Ratings & comments	We store this so the user can see a history of his actions inside the app.	Firestore and Super admin

	Payment details	BankID, firstname, last name, personal number*/d number,* bank account number Address (City, Country, Postal* code, Street*)	To provide business with valid payment details for Staffer. And to send to our third provider so they can handle the payment for jobs done. We at Staffers AS do not see personal number/d-numbers. We only see bank accounts for a limited time, if you refer to another worker/company. This is so we can payout your reward. After the reward is paid out, we do not have access to it anymore.	Firestore and Super admin *Is only for Firestore Bank account nr (limited time)

	Jobs	Job detail (Company name, Description, Type, Hourly wage, Start and End date)	We store information about each job created by the manager so the staffer has all relevant information to apply.	Firestore and super admin
	Business profile information	Address(City, Country, Postal code, Street - GPS coordinates), Business name, Business type, coordinates, Description, Phone, Jobs created, Ratings, Org. number, Payout day	Manager can fill out information about his real business so staffers can apply to jobs that have been created under the business name. Staffers AS use this for improval purposes and for sending invoices.	Firestore Super admin

	Messages	Message history	To show users their message history. Staffers AS do not have access to the chat	Firebase
	Staffers contract	Staffer name, Business name, business address, staffer personal id, business org nr, salary, date, working hours, staffers address, salary payout date	This is the contract between the staffers and company to be able to do the jobs applied for. We at Staffers AS do not see this contract	Firestore
	Access and apply	Personal ID (Driving license or passport) and tax card and BankID	To ensure that the people that work for businesses have legally working rights in Norway. We only see personal ID and tax card for a limited time. When uploading it, we at Staffers AS decline or accept it. After this action is taken, we do not have access to the documents anymore. To make this process as efficient as possible, we have made an own section where people that upload these documents are listed.	Firestore Superadmins (Limited time)

Appendix B - Terms of the Data Processor's use of sub-processors and list of approved sub-processors

General consent

The Data Controller has the users general consent for the engagement of sub-processors. The Data Controller shall, however, inform the users of any planned changes with regard to additions to or replacement of other data processors and thereby give the Data Controller the opportunity to object to such changes. If the Data Controller should object to the changes, the Data Controller shall notify the users of this within ten (10) days of receipt of the notification. The users shall only object if the Data Controller has reasonable and specific grounds for such refusal. Any qualified risk of infringement of the privacy rights of the data subjects shall always be deemed as reasonable and specific grounds for refusal.

Approved sub-processors

The Data Controller shall on commencement of this Data Processing Agreement approve the engagement of the following sub-processors:

Name	**CVR no.**	**Address**	**Description of processing**	**Country of processing**
Google Inc	602223102	300 DESCHUTES WAY SW STE 304, TUMWATER, 985010000, WA	To collect standard google analytics for the website	Global, At your region*
Apple Inc		One Apple Park Way, Cupertino, California, USA, 95014	To setup/login as a user	Global, At your region*

** "Global, At your region", means that the provider stores your personal data in the nearest server to your country in your region, for example EU.*