&frankly and GDPR

Table of contents

1. The purpose of this document

The purpose of this document is to explain how Andfrankly Pulse AB (hereinafter called "&frankly") complies with applicable data protection legislation, in particular with the EU General Data Protection Regulation ("GDPR"), when providing its service to its customers. This document describes which personal data &frankly handles, how &frankly meets the legal requirements in its capacity of personal data processor ("Processor"), and how we assist our customers in their capacity of personal data controllers ("Controllers") using our service.

This document is provided as an overview and is subject to changes (i) as we continue to develop the service and (ii) in order to reflect compliance with legislative changes. This document is not a comprehensive overview of GDPR as such, but rather highlights specific requirements which apply to customers' use of our service and how we assist in meeting them.

2. Background

Safeguarding customer data, including the personal data we process for our customers, is a key business priority for &frankly. Our reputation as a service provider is based on trust that we will handle personal data in a secure and responsible way. It is also an explicit legal requirement on us in our capacity of Processor.

&frankly has prior to the introduction of GDPR, complied with the Swedish personal data Act (1998:204) ("PUL"), which is based on the EU Directive 95/46/EC and aimed at preventing the violation of personal integrity in the processing of personal data. As a service created under already strict data protection legislation, &frankly has already before the introduction of GDPR been designed with high privacy in mind.

GDPR entered into force on 25 May 2018, and &frankly has since had to comply with GDPR in addition to other applicable data protection legislation. This document contains information on our compliance with GDPR and how we can assist our customers, in their capacity of Controllers, to comply with GDPR while using our service.

3. Data collected and processed

&frankly processes *direct* personal data of our customers' employees such as first and last name, email-address, their position in the organizational structure and other employee-related attributes to the extent provided to us by our customers. &frankly also stores structured logs of activities performed by the employees in the application for troubleshooting purposes, and traffic logs containing IP addresses in unstructured log files. Employees may voluntarily provide &frankly with a profile picture and location data to personalize their use of the service, unless it is disabled by the customer. &frankly also stores and processes *indirect* personal data such as responses to questions asked ("Response Data"), until such data is disconnected from the individual by de-identification.

If our customers have enabled the Whistleblower functionality, we may also process personal data of other persons that choose to submit Whistleblower reports through the publicly accessible whistleblower reporting page. The personal data processed in this function is contact details to the reporter (name and optionally email and phone number), and any personal data the reporter decide to provide in the case report. The lawful basis of processing personal data of Whistleblower cases is typically the legal requirement of the company to do so, and the reporter is provided with information upon reporting (link to the public information page https://www.andfrankly.com/en/information-to-employees/). Whistleblower reports are kept for 2 years and then automatically pruned of personal

data, or the report can be deleted directly by the company in our service upon need to remove personal data.

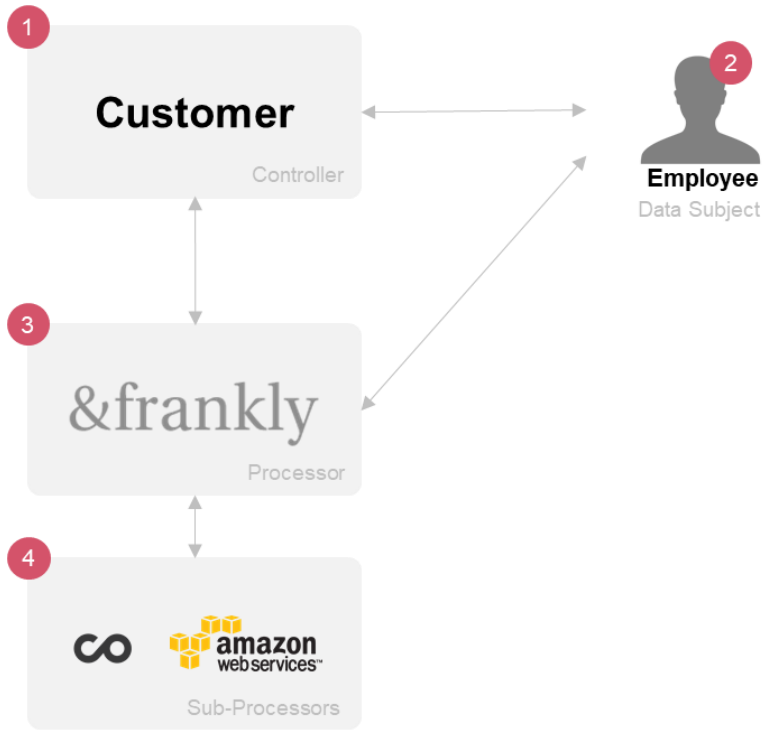
Personal data processed by &frankly is structured and stored in a database or in structured logs. Employees can however also provide free text comments in the service where, if personal data is supplied, such data is stored in an unstructured form. Customers are explicitly disallowed to use the service in a manner that would result in processing of any sensitive data (e.g. race, sexual preference etc.).

Data processed	**Notes**
First name	
Last name	
Email	
Phone	Optionally if enabled by customer to use as means of authentication, by default disabled.
Location (GPS)	Optionally provided by employees in app, can be disabled.
Profile picture	Optionally provided by employees in app, can be disabled.
Organizational belonging	E.g. position in the organizational structure, manager responsibility of team, depending on customers desired use of the service.
Account settings	Preferences employee has chosen, e.g. frequency of notifications, choice of notification channels, out of office setting, choice of language in the application, time zone to use for notification time.
Response Data	Answers to questions asked in the service, data depends on questions asked. Note that this data is only considered personal data until it is anonymized / no longer linked to the employee.
Actions Data	Actions taken by the employee that they have decided to track in &frankly. Either which standard action we or the customer proposed they signed up to, or details of a custom created Action that they defined themselves. This feature is optional and can be disabled.
Additional employee data	Provided by the customer at their discretion to provide ability to slice results. Examples can be *Country*, *Employment length span*, *Age span*. This feature is optional and can be disabled
Application activities	Activities performed in the application, logged to provide traceability of changes and for troubleshooting purposes. Stored as structured data consisting of Who, What, When e.g. *User X*, *Created Group Z*, *Time: 2018-03-05 12:00*.
Support & customer satisfaction data	Answers to our questions we send directly to end users about their satisfaction of our service, including follow-up questions asking for feedback on what to improve. Gathering of this data can be disabled on request to our support. Support ticket information (name, email, issue details, incident history) linked to the individual who initiated/is involved in the ticket.
Traffic logs	Containing IP-addresses and pseudonymized user identifiers for troubleshooting purposes, but no other personal data.

Device metadata	Browser and operating system version, timezone & language settings and similar user agent details or technical capabilities (e.g. platform versions, library versions) that is provided implicitly by browsers or by operating system to apps, used to add additional context to e.g. support tickets or application activity.
Whistleblower reports	Report details for whistleblower repors that may contain personal data in unstructured text.

4. Data flow

Below is a high-level data flow for personal data in the service, with legal persons as denominated in GDPR involved and their roles with respect to the service.



1. **Controller** – Our customers are always Controllers of the personal data processed by &frankly in their use of our service, as they defined the purpose of its use and have elected &frankly as the means. They own and are responsible for the data processed by us. Typically, customers provide &frankly with *direct* employee data (first- and last name, email, position in the organizational structure, as well as other attributes coupled to the employee that the customer desires we handle for results slicing). This personal data is in turn typically provided to the customer by the employees (Data Subjects) to handle their employment in the company.

2. **Data Subjects** - The customers' Employees (which may include employees from other companies whose personal data the Controller has rights to handle as defined in our Personal data processor Agreement) are Data Subjects, whose personal data we process. The employees provide data to the customer and/or their employer (if another company than the customer), but also directly to &frankly when answering questions (Response Data) or when

providing voluntary account information (profile picture, location, account settings). Activities performed in the service also generate personal data stored for each Data Subject.

3. **Processor** - &frankly is Processor for our customers and may only process the data in accordance with instructions provided and in accordance with our Personal data processor Agreement and applicable data protection legislation. &frankly uses the personal data to provide its service (handle users and groups, ask questions, process & present results). &frankly provide personal data back to the customer (e.g. user lists, show organizational structure) and to the individual employees as part of the use of our service (e.g. employees' own results, their individual settings) as well as upon data-requests from the employee (approved by the customer), but is obliged to never provide individual Response Data to the customer under our agreement with the customer and in order to protect the privacy of employees providing answers to questions in the service.

4. **Sub-Processor(s)** - &frankly utilizes Sub-Processors to deliver its services, and a list of them and what data they process can at all times be found here: https://www.andfrankly.com/en/gdpr-subprocessors/. &frankly has a Data Processor Agreement with all of our sub processors. Our main sub-processor is Amazon Web Services that we use for our own infrastructure, and where the data that &frankly receives is stored. Other sub-processors than AWS only process subsets of personal data (such as email, IP-address – never answers to questions). In some cases, for example for emails & IP-addresses, they may process such data outside of EU/EEA but in such cases may only do so in compliance with our Data Processor Agreements and GDPR including meeting necessary data protection requirements that GDPR prescribe for transfers out of EU/EEA, including under Standard Contractual Clauses. &frankly utilizes other suppliers in providing its services, but do not provide these suppliers with any personal data received from the customer.

6. Purpose of data collection, consent and information to employees

Different companies use &frankly for different purposes, and each customer define their own purpose for their use of our service and the processing of personal data in it. That said, unless it is specified otherwise towards employees or in the instructions given to us for personal data handling, &frankly's standard agreements provides the following purpose as a starting point:

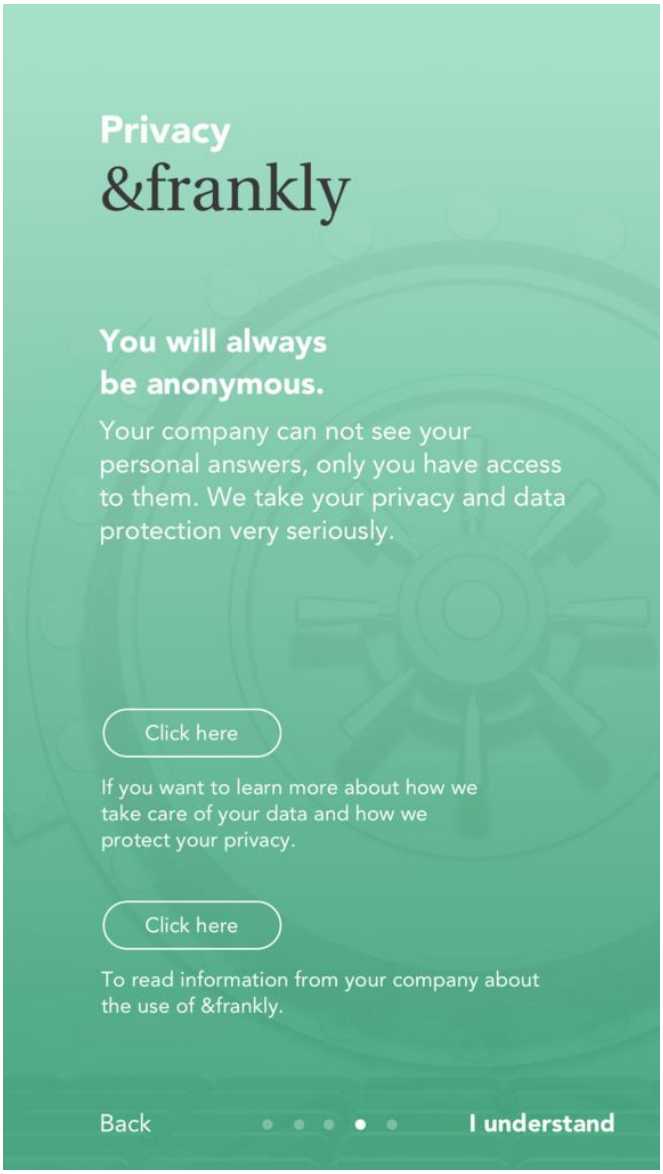
The Company's purpose, for which it has chosen to use the service is to increase the Employees' influence and commitment and thereby improve the Company's working conditions and business ("the Purpose").

Under GDPR personal data shall be collected for specific, explicit and legitimate purposes, and individuals whose personal data is processed should be provided information about it in a clear and easily accessible form. It is therefore important that each customer defines the purpose for which they use &frankly and communicate this to its employees. This can be done during the onboarding process in &frankly (see below).

While customers may well consider that collection of personal data for use in &frankly's service refers to such personal data that is of legitimate interest for the customer to collect as part of an employment or otherwise not requiring the employees' consent[1], we advocate to collect consent from the employees for personal data collected and processed by &frankly. Doing so also ensure that employees understand what &frankly is about, and why the company has decided to use the service.

[1] See GDPR article. 6 1 (f), and specifically for activity and traffic logs coupled to recital 49

&frankly provides means for our customers to inform employees and obtain their consents in order to collect and process their personal data for our service in the application during first login:



During this step, customers can include a link to own material that clarifies the purpose of processing, explicitly collects additional consent, if needed, for the use of our service, describe customer-specific data that will be processed and provide general information about &frankly. &frankly will store the employees' confirmations in our database as a record.

In addition to the above, &frankly provides an *Information for Employees* page[2] that describes the rights of employees and information about how they can invoke said rights in relation to the service. This page also provides an overview of how individual data is being handled, and how the privacy of employees' answers is protected.

It should be noted that the employees are always able to freely choose if they want to answer questions in &frankly and hence have full control over which personal data is being stored and

[2] https://www.andfrankly.com/en/information-to-employees/

processed by us in addition to the direct personal data (name, email and position in the organizational structure) that the customer supplies us with.

Note that for Whistleblower reporting functionality, the lawful basis of processing may be referenced as the legal requirement for the company to process such data.

6. Data storage, processing and transfer

Personal data in the &frankly service is stored and processed within EU/EEA, specifically in AWS datacenters located in Frankfurt, Germany. Sub-processors may process specific information outside of EU/EEA, such as email or IP-addresses but in such cases only in accordance with Data Processor Agreements and Standard Contractual Clauses as per the requirements set forth in GDPR for such transfers, and as ruled valid in the Schrems II ruling.

Personal data may also be manually processed by &frankly staff in Stockholm, Sweden, but in such circumstances primarily transiently, e.g. while being imported into our system, and is not to be retained locally after import/use. It is strongly recommended that customers only provide personal data into our system directly and avoid sending personal data though e.g. email.

&frankly may on customer's request transfer results data for analysis to another party (e.g. a company which can provide analysis services on the data). In such cases only anonymized data that does not include personal data is transferred. In order to perform such a transfer, a specific data transfer agreement must be signed by the customer, &frankly and the hired company, to ensure complete protection of anonymity of the data subject and their answers.

6.1 On location of data processing and Schrems II

Following the Schrems II ruling and the recommendations around additional safeguards required for transfer of personal data to third countries from EDPB, &frankly has reduced the number of sub-processors based in third countries and the amount of personal data we need to send to such sub-processors. We have also ensured that all data processing agreements include Standard Contractual Clauses that Schrems II maintained were still valid.

A few of the sub-processors we continue to use and who are based in the United States are necessary for us to deliver our service, and such we do not have the possibility to replace immediately. We have made the assessment taking into account available technology, the implementation costs and the nature, scope, context and purpose of the processing, as well as the risks, that we may continue to handle personal data with these sub processors.

The background to this is that:

1) the data they process constitutes a subset and less sensitive / typically commonly spread part of our customers' personal data; for example email and first name - never answer to questions or detailed information about the individuals such as gender, date of birth or the like;

2) in our data processing agreements with these sub-processors, and in how the technical solution is set up with these them, we ensure that personal data is handled confidentially and with strong security (including encryption during storage and transfer and, where it is possible, on servers in the EU/EEA. Most of our US sub-processors are also based in California and are subject to the California Consumer Privacy Act, which imposes requirements on the handling of personal data that in many respects reflect the GDPR). Several sub-processors have also given guarantees that they will object to extraction requests for personal data processed in their service if requested by e.g. the US government.

For customers that wish to use &frankly and ensure that processing is strictly limited to EU/EEA, we will per August 2021 offer a "***Reduced processing***" mode that can be enabled on your &frankly account. When enabled, we will restrict processing of your personal data to within EU/EEA by disabling our use of sub-processors that process personal data outside of EU/EEA. Which sub-processors that will no longer be used when this mode is enabled can be seen on the https://www.andfrankly.com/en/gdpr-subprocessors/ page.

Note that with "***Reduced processing***" enabled, our ability to provide full level of support and troubleshooting is constrained. Specifically, we will have less visibility into your account in our Customer Success and Support functions, will not include your account in customer satisfaction surveys and we will have less information to go on for technical troubleshooting through our analytics and error logging. If you want to completely restrict users sending emails to our help function that could be processed outside of EU/EEA we can also disable our help@andfrankly.com email for your specific domain – please contact us if you wish to do so.

We continue to follow the development of handling of personal data outside of EU/EEA after the Schrems II ruling, and will evaluate and be prepared to act if there are indications that we have to make additional changes, including continued evaluation of moving ALL handling of parts of our service within the EU whenever possible.

7. Data retention and pruning/removal

&frankly retains personal data that our customers provide us for as long as we provide the service under our agreement with the customer. Upon termination of the service, personal data is returned to the customer if requested (in which Response Data is anonymized) and personal data is permanently removed from the service and &frankly.

Personal data of employees is removed and its link to Response Data is removed in the service 30 days after the customer removes said employees from the service by manual edit/deletion, automatic edit/deletion via integrations and/or when an employee requests that personal data be removed as set forth in GDPR.

In order to reduce the amount of personal data stored in &frankly and comply with GDRPs principle of limiting data collection to what is necessary, it is recommended that customers continuously prune the employees managed in &frankly, preferably by using one of the means we provide to handle employees automatically. Using automated means of managing employees also ensures that customers can comply with the GPDR principles of always making sure that personal data is accurate and up to date.

Logs that are stored as unstructured data and may contain personal data (e.g. IP address and/or pseudonymized user id) is retained for 60 days for auditability/security purposes, and then permanently removed.

Personal data in backups may be stored for 30 days for data security/availability reasons, after which backups are permanently removed.

Whistleblower reports are kept for 2 years and then automatically pruned of personal data, or the report can be deleted directly by the company in our service upon need to remove personal data.

8. Right to access, right to be forgotten and individual rights

Under GDPR employees shall be provided mechanisms to request, rectify and erase personal data about them, and such mechanisms shall be possible to access electronically if processed by electronic means. Requests shall be handled in a timely manner, and individuals shall also be able to request data stored about them on a structured format that is machine-readable and interoperable.

&frankly provides employees and our customers with such means in several ways, described in our user guides and in our *Information for Employees*:

- Employees may at any given time see information stored about them through our application (i.e. individual results to questions asked, individual settings)
- Customer administrators may at any time see the basic personal data about employees and make corrections to such information by functions in our application, including remove individual employees and their personal data (user & group views).
- For access to data, corrections and/or erasures which cannot be made directly in our application, employees may always request assistance from our help desk via help@andfrankly.com[3].
- For requests of access to data in a structured/interoperable format, we provide the employee with such data structure in e.g. CSV or JSON plain text formats upon request.

Furthermore, our *Information for Employees* provides concise and clear information about the rights that employees have in relation to their personal data, and how they can invoke these rights in their use of &frankly.

9. Data security and Data protection

Under GDPR personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

&frankly employs a broad number of technical and organizational measures to protect the confidentiality, integrity, availability of data, as well as auditability. On request we can provide additional documentation to customers that demonstrate how we provide data security and comply with said requirements:

- **&frankly - Information Security Policy & Procedures** – Documentation regarding the Information security policies which &frankly follows, as well as the procedures employed for e.g. Incident-, Problem-, Configuration- and Change Management, Business Continuity, Security Management, Secure Development etc., i.e. organizational measures taken to manage information securely.

- **&frankly – Solution overview** – Documentation describing our overall technical solution as well as technical security controls and measures taken to protect information confidentiality, integrity, availability and auditability.

[3] Note that any request for personal data sent to &frankly is always confirmed with the respective customer in their capacity of Controllers.

For parts of our platform which we do not manage ourselves (e.g. our infrastructure, currently provided by Amazon Web Services[4]), we only will choose suppliers meeting high standards as to data protection and security and can provide compliance/certification with e.g. ISO 27001 or similar.

Under GDPR data protection shall be *by design* and *by default*. &frankly was designed from the ground up with individual privacy and data protection in mind. By default, we only require the minimum of data necessary to provide our service; employee name and email-address. At any given time, it is up to the employees and customers to provide us with any additional data; such as preferences, location or profile picture– as well as answers to questions asked in our service. Employees are always in control of which response and account settings data they share with us in their use of the service. We provide employees with the means to see all own answers they have given in the service, and hence the total set of data we store about them. Along with very simple means to contact us: help@andfrankly.com, employees may choose to provide as little or much information as they would like to &frankly – and also at any time see which personal data belonging to them we store, and contact us for requests to correct/remove or export it.

In our *Solution overview* we provide details on the security mechanisms we employ to secure data by design: encryption at rest and in transit, authentication and access controls, firewalls and intrusion detection/prevention, and much more.

10. Responsibility and Data processing obligations

The responsibilities of customers and &frankly in processing of personal data used in our service is outlined in detail in our *Personal data processor Agreement* which, together with General conditions for the Service, is an integral part of our Service Agreement with our customers and has been specifically created to comply with GDPR.

The said documentation, this document, and the auxiliary documentation mentioned throughout this document as a collection provide comprehensive information to our customers in demonstrating compliance with GDPR. In addition, and under our Personal data processor Agreement, customers may perform audits and/or request additional information from us as necessary to demonstrate compliance with GDPR.

&frankly has a designated data protection officer who is member of the management team of the company. This person is tasked with protection of data stored in &frankly, including personal data, and is also responsible for maintenance and implementation of our information security program.

11. More information

If you would like more information about &frankly and/or how we handle and protect personal data, please contact us at hello@andfrankly.com and we are happy to provide it! If already are a customer, please reach out to our customer success team via help@andfrankly.com for questions.

[4] See more about AWS Cloud security at https://aws.amazon.com/security/