Ada Health GmbH Privacy Policy – Employees/ Applicants

For the candidates who apply for the UK-based positions, please scroll down to read the Ada Health UK Privacy Policy – Employees/ Applicants.

Protecting your data, privacy and personal data (as defined under Article 4(1) of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**")) is very important to Ada Health GmbH ("**Ada**", "**us**", "**our**" or "**we**"). With this privacy policy (the "**Privacy Policy**"), we want to inform you how we process your data for the establishment, performance and termination of your employment contract according to Article 13 and 14 GDPR.

1. Ada as Data Controller

This Privacy Policy applies to any personal data processed by Ada Health GmbH (HRB 189710), Neue Grünstraße 17, 10179 Berlin, Germany being the data controller (as defined under Article 4(7) GDPR) of all processing activities in connection with your job application or employment.

During your employment you are not subject to automated decision making. Where the legal basis for processing your data is indicated as performance of your work contract you are contractually obligated to provide your data. Where it is indicated as compliance with a legal obligation, you are legally required to provide your data. In all other cases, provision of your personal data is voluntary.

Questions, comments and requests regarding this Privacy Policy are welcome and should be addressed through a ticket in the Legal and DPO Service Desk. Our data protection officer can be contacted directly at dpo@ada.com or via Slack

2. Which personal data we may collect and process, why and for how long

2.1 Job application/ Recruitment

- *Types of data:* first name, last name, email address, phone number, geographic location (city), resume, LinkedIn profile (optional), time and date of the application.
- *Purpose of processing:* If you are an applicant on our website, apply via email through third party platforms such as LinkedIn, we may process

the above data in order to check your suitability for the position (or any other vacancies within our company) and to conduct the application process.
- *Use justification:* To take steps at your request prior to entering into a contract (Article 6(1)(b) GDPR and § 26 (1) BDSG).
- *Storage duration*: In the event of a rejection, candidate data will be deleted after 6 months. If you have agreed to further storage of your personal data, we will add your data to our applicant pool. The data will be deleted after two years from that moment. If you are offered a job in the context of the application process, the data from the data system will be transferred to our Human Resources information system.

2.2 Onboarding

- *Types of data:* Contact details (Email address, home address, phone number), name, date of birth/ age, city of birth, country of birth, nationality, location, gender, marital status, social security information: tax number, social security number, tax class, health insurance, existence of secondary activities, children name and birthdate, work permit, payment data (IBAN / Sort Code), employee's Bamboo number; handicap, pregnancy status, religious affiliation
- *Purpose of processing:* We process your data to integrate you into Ada as a company. This includes setting up the required contracts and other declaration, setting up your salary payments, providing you with equipment you might need as well creating accounts for software tools you need to use.
- *Use justification:* Performance of your employment contract (Article 6(1)(b), 9(2)(b) and § 26 (1) BDSG)
- *Storage duration:* We store your data until the end of your employment. We might store some of the data for a longer time if it is needed for the fulfilment of a legal obligation or defence against legal claims.

2.3 Performance of Work

- *Types of data:* Email address, name, location, Gender, technical identifiers, work results
- *Purpose of processing:* We process this data to enable the performance of your work duties and the results and products of your work as owed under your employment contract.
- *Use justification:* Performance of your employment contract (Article 6(1)(b), and § 26 (1) BDSG)

- *Storage duration:* We store your data until the end of your employment. We might store some of the data for a longer time if it is needed for the fulfilment of a legal obligation or defence against legal claims. To the extent that your personal data form part of the work product we do not delete it.

2.4 Payroll

- *Types of data:* Tax number, social security number, tax class, health insurance, existence of secondary activities, children name and birthdate, work permit, payment data (IBAN / Sort Code), religious affiliation
- *Purpose of processing:* We process your data to facilitate payment of your salary as well as other payments owed (e.g. Reimbursements)
- *Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR, and § 26 (1) BDSG), compliance with a legal obligation (Article 6(1)(c) GDPR)
- *Storage duration:* We will retain accounting data in accordance with the commercial and tax law storage obligations of six or ten years (§ 147 German Tax Code, § 257 German Commercial Code).

2.5 Work time management

- *Types of data:* Name, sick note, hours worked, potential causes for illness (only when risk of infections for other employees)
- *Purpose of processing:* We process your data to manage your worktime. For regular employees this means managing your regular leave times, your time spent working from abroad as well as your sick leave. This also includes managing absences company wide and communicating those to the relevant teams. For employees paid on an hourly bases we also process your data to calculate your salary.
- *Use justification:* Performance of your employment contract (Article 6(1)(b), 9(2)(b) and § 26 (1) BDSG)
- *Storage duration:* We will retain your work time management data according to applicable legal retention obligations of 4-7 years for records of working hours and 7 years for sick leave data.

2.6 Employee retention management (office parties, offers, etc.)

- *Types of data:* Name, email address

- *Purpose of processing:* We process your data to plan and execute company events such as office parties, to provide you with special offers (e.g. Gym, company bike, etc.).
- *Use justification: Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR and § 26 (1) BDSG)
- *Storage duration:* We store your data until the end of your employment.

2.7 Travel Management

- *Types of data:* Name, email, home address, passport data (passport no., date of issuance/ expiration, etc.)
- *Purpose of processing: We process your data to organize business trips on behalf of existing employees or travel to a job interview at Ada for applicants.*
- *Use justification:* Use justification: Performance of your employment contract (Article 6(1)(b) GDPR and § 26 (1) BDSG)
- *Storage duration:* Your data will be stored for the duration necessary to comply with legal and contractual requirements resulting from the trip.

2.8 Internal use of personal data

- *Types of data:* Name, email, photo (where applicable)
- *Purpose of processing:* We process your data to create to enable company-wide communication and interaction that is not strictly work related. The use of certain data might be subject to your consent (e.g. your photo).
- *Use justification:* Our legitimate interest (Article 6 (1)(f) GDPR to create a positive and enjoyable work environment for our employees as well as your consent (Article 6(1)(a) GDPR)
- *Storage duration:* We store your data until the end of your employment. We will delete data that we process based on your consent when you revoke it.

2.9 Use of personal data on website

- *Types of data:* Name, email, photo (where applicable)
- *Purpose of processing:* We process your data to present our work and our key personnel on our website and present relevant contact points. The use of certain data might be subject to your consent (e.g. your photo).
- *Use justification:* Our legitimate interest (Article 6 (1)(f) GDPR to present our work in useful manner and make ourselves available for being contacted as well as your consent (Article 6(1)(a) GDPR).

- *Storage duration:* We store your data until the end of your employment. We will delete data that we process based on your consent when you revoke it.

2.10 Enforcement of pandemic restrictions

- *Types of data:* Name, vaccination status (number and data of vaccination), antigen test result (where applicable)
- *Purpose of processing:* We process your data to comply with possible pandemic restrictions such managing access to the office applicable to employers. Depending on the applicable regulations and guidelines, we might be required to check your vaccination status or quick test results upon entry to the office or other work-related gatherings.
- *Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR, and § 26 (1) BDSG) or fulfilling a legal obligation (Article 6(1)(c) GDPR).
- *Storage duration:* We do not store data on your vaccination status or test results unless you have given us consent to do so. In this case, we delete your data when you revoke your consent or when the legal test requirement does not longer apply.

2.11 Temporary employment

- *Types of data:* See description of processing purposes in this section 2 above
- *Purpose of processing:* If you work for Ada as a temporary employee, your direct employer is the temporary employment agency. The data processing as described in this section 2 is carried out both by the temporary employment agency and by Ada as controllers. Ada may not carry out all of the aforementioned processing steps itself, but rather the temporary employment agency according to its own privacy policy.
- *Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR and Section 26(1) BDSG) or compliance with a legal obligation (Article 6(1)(c) GDPR), unless otherwise stated in the individual processing activities.
- *Storage duration:* We store your data until the end of your employment. We may retain some of the data for longer if it is required to fulfil a legal obligation or for the defence of legal claims. If your personal data is part of the work product, we will not delete it.

3. Where do we store your personal data

The personal data that we collect from you is generally stored in the European Union on Cloud Servers of Amazon Web Services EMEA S.A.R.L. (“AWS”) with a business seat in Luxembourg and on the Cloud Servers of Google Commerce Limited ("GCL"), a company incorporated under the laws of Ireland, with its offices at Gordon House, Barrow Street, Dublin 4, Ireland. This data may, however, be processed by sub-processors operating outside of the European Economic Area (“EEA”), namely the USA, based on a data processing agreement.

4. Disclosure of your personal data

4.1 We use technical service providers to operate and maintain our Services, who act as our processors based on a data processing agreement. Where we use Service providers who process personal data on our behalf outside the EEA (or “**third countries**”) we do so with the appropriate safeguards for your data subject rights. For all our service providers we either rely on an applicable adequacy decision (for the US this is currently the EU-US Privacy Framework) or include the standard contractual clauses in our data processing agreements.

4.2 In addition, we do not transfer your personal data to third parties - with the exception, when applicable, of the purposes listed below

- *Use justification:* The legal basis for the transfer and processing of your personal data by the processor corresponds to the legal basis on which we, as data controller, rely (always in compliance with section 3 above).

4.3 If we sell or buy any business or assets, we may disclose your personal data to the prospective seller or buyer of such business or assets.

- *Use justification:* Legitimate interest (Article 6(1)(f) GDPR): to sell our business or assets / where required by applicable law: consent (Article 9(2)(a) GDPR): for the processing of special categories of data, i.e. your personal health data.

4.4 If we or, substantially, all of our assets are acquired by a third party, personal data about our users will be one of the transferred assets.

- *Use justification:* Legitimate interest (Article 6(1)(f) GDPR): to sell our company or assets / where required by applicable law: consent (Article 9(2)(a) GDPR): for the processing of special categories of data, i.e. your personal health data.

4.5 If we are required on the basis of EU law or the law of a Member State to disclose or share your personal data.

- *Use justification:* Legal obligation (Article 6(1)(c) GDPR).

5. How long do we retain your personal data

We will hold your personal data for as long as it is necessary or required by law or by any relevant regulatory body, and always in compliance with the data minimization principle. Specific storage periods for the respective processing activities are detailed in section 3 above.

If your personal data is used for more than one purpose, we will retain it until the purpose with the longest period expires, but we will stop using it for the purpose with the shorter period as soon as the shorter period expires (to comply with the purpose limitation principle). We restrict access to your personal data to the persons who need to use it for the relevant purpose(s), always in compliance with the integrity and confidentiality principle.

After the processing of your data is no longer necessary for the purposes outlined in section 3 we will securely and separately store some of your data in accordance with statutory retention obligations applicable to us and reasonable business needs.

The retention period for the majority of your data ends when your employment with Ada is terminated. However, this does not mean that your data will be deleted at this point. The deletion period will often be longer, e.g. we will keep your personnel file for 3 years after the end of your employment.

Please be aware, that Ada will not delete data that is considered to be an owed work result by you. This might extent to any creation attributable to you, your communication with other employees (emails, Slack messages, etc.), comments, presentations, photo/video recordings, etc.

6. Your data subject's rights

Under GDPR you have various rights in relation to your personal data (as listed below). All of these rights can be exercised by contacting us via our contact form, by selecting "Exercising My Data & Privacy Rights".

- **Right to withdraw consent**: Where the processing of your data relies on your prior consent, you have the right to withdraw such a consent at any time by notifying us via email at dpo@ada.com. By withdrawing your

consent, the lawfulness of the processing based on consent up until the point of withdrawal will not be affected.

- **Right to object**: As a data subject, you have the right to object on grounds relating to your particular situation, at any time, to the processing of your personal data which is based on Article 6(1)(f) GDPR ("legitimate interest" as indicated above) including profiling based on those provisions. In the event of an objection relating to your particular situation, we will no longer process your personal data, unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.
- **Right to be informed**: As a data subject, you have a right to obtain access and information under the conditions provided in Article 15 GDPR. This means in particular that you have the right to obtain confirmation from us as to whether we are processing your personal data or not. If so, you also have the right to obtain access to the personal data and the information listed in Article 15(1) GDPR. This includes information regarding the purposes of the processing, the categories of personal data that are being processed, and the recipients or categories of recipients to whom the personal data have been or will be disclosed.
- **Right to erasure / 'Right to be forgotten'**: As a data subject, you have a right to erasure ("right to be forgotten") under the conditions provided in Article 17 GDPR. This means that you generally have the right to obtain from us the erasure of your personal data and we are obliged to erase your personal data without undue delay when one of the reasons listed in Article 17(1) GDPR applies. You can do this by deleting your account, in the App, at any time. If we have made the personal data public and are obliged to erase it, we are also obliged, taking account of available technology and the cost of implementation, to take reasonable steps, including technical measures, to inform controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of those personal data (Article 17(2) of the GDPR. The right to erasure ("right to be forgotten") does not by exception apply if the processing is necessary for one of the reasons listed in Article 17(3) GDPR. This can be the case, for example, if the processing is necessary for compliance with a legal obligation or for the establishment, exercise or defense of legal claims (Article 17(3)(b) and (e) GDPR).
- **Right to restriction of processing**: As a data subject, you have a right to restriction of processing under the conditions provided in Article 18 GDPR. This means that you have the right to obtain from us the restriction of processing if one of the conditions provided in Article 18(1)

GDPR applies. This can be the case, for example, if you contest the accuracy of the personal data. In such a case, the restriction of processing lasts for a period that enables us to verify the accuracy of the personal data (Article 18(1)(a) GDPR). Restriction means that stored personal data are marked with the goal of restricting their future processing (Article 4(3) GDPR).

- **Right to data portability**: As a data subject, you have a right to data portability under the conditions provided in Article 20 GDPR. This means that you generally have the right to receive your personal data with which you have provided us in a structured, commonly used and machine-readable format, and to transmit those data to another controller without hindrance from us where the processing is based on consent (pursuant to Article 6(1)(a) or Article 9(2)(a) GDPR or on a contract (pursuant to Article 6(1)(b) GDPR), and where the processing is carried out by automated means (Article 20(1) GDPR). In exercising your right to data portability, you also generally have the right to have your personal data transmitted directly from us to another controller where technically feasible (Article 20(2) GDPR).
- **Right to Rectification**: As a data subject, you have the right to rectification under the conditions provided in Article 16 GDPR. This means in particular that you have the right to receive from us, without undue delay, the rectification of inaccuracies in your personal data and completion of incomplete personal data.
- **Right to complain**: As a data subject, you have a right to lodge a complaint with a supervisory authority under the conditions provided in Article 77 GDPR. The supervisory authority responsible for us is the Berlin Data Protection Authority in Germany (*Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Address: Friedrichstr. 219, 10969 Berlin; Telephone: 030 13889-0; E-Mail: mailbox@datenschutz-berlin.de).

7. Changes to this policy

Any changes we make to our Privacy Policy in the future will be posted on this page, and where appropriate, notified to you by email, or by any other available means. We therefore encourage you to review it from time to time to stay informed about the way we are processing your data.

Last updated: July 5th, 2024

****

Ada Health UK Privacy Policy – Employees/ Applicants

Protecting your data, privacy and personal data (as defined under Article 4(1) of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**")) is very important to Ada Digital Health Ltd. ("**Ada**", "**us**", "**our**" or "**we**"). With this privacy policy (the "**Privacy Policy**"), we want to inform you how we process your data for the establishment, performance and termination of your employment contract according to Article 13 and 14 GDPR.

1. Ada as Data Controller

This Privacy Policy applies to any personal data processed by Ada Digital Health Ltd., Duke Street 33, 4th Floor, London W1U 1LH, England United Kingdom (ICO Registration: ZA218767) being the data controller (as defined under Article 4(7) GDPR) of all processing activities in connection with your job application or employment.

During your employment you are not subject to automated decision making. Where the legal basis for processing your data is indicated as performance of your work contract you are contractually obligated to provide your data. Where it is indicated as compliance with a legal obligation, you are legally required to provide your data. In all other cases, provision of your personal data is voluntary.

Ada engages its parent company, Ada Health GmbH (HRB 189710), Neue Grünstraße 17, 10179 Berlin, Germany as its data processor for large parts of the processing described in this Privacy Policy based on a data processing agreement. The EU is considered to provide an adequate level of data protection under UK privacy law. Any reference to Ada in this Privacy Policy shall also include Ada Health GmbH.

Questions, comments and requests regarding this Privacy Policy are welcome and should be addressed through a ticket in the Legal and DPO Service Desk. Our data protection officer can be contacted directly at dpo@ada.com or via Slack.

2. Which personal data we may collect and process, why and for how long

2.1 Job application/ Recruitment

- *Types of data:* first name, last name, email address, phone number, geographic location (city), resume, LinkedIn profile (optional), time and date of the application.
- *Purpose of processing:* If you are an applicant on our website, apply via email through third party platforms such as LinkedIn, we may process the above data in order to check your suitability for the position (or any other vacancies within our company) and to conduct the application process.
- *Use justification:* To take steps at your request prior to entering into a contract (Article 6(1)(b) GDPR).
- *Storage duration*: In the event of a rejection, candidate data will be deleted after 6 months. If you have agreed to further storage of your personal data, we will add your data to our applicant pool. The data will be deleted after two years from that moment. If you are offered a job in the context of the application process, the data from the data system will be transferred to our Human Resources information system.

2.2 Onboarding

- *Types of data:* Contact details (Email address, home address, phone number), name, date of birth/ age, city of birth, country of birth, nationality, location, gender, marital status, social security information: tax number, social security number, tax class, health insurance, existence of secondary activities, children name and birthdate, work permit, payment data (IBAN / Sort Code), employee's Bamboo number; handicap, pregnancy status, religious affiliation
- *Purpose of processing:* We process your data to integrate you into Ada as a company. This includes setting up the required contracts and other declaration, setting up your salary payments, providing you with equipment you might need as well creating accounts for software tools you need to use.
- *Use justification: Performance of your employment contract (Article 6(1)(b), 9(2)(b)*
- *Storage duration:* We store your data until the end of your employment. We might store some of the data for a longer time if it is needed for the fulfilment of a legal obligation or defence against legal claims.

2.3 Performance of Work

- *Types of data:* Email address, name, location, Gender, technical identifiers, work results

- *Purpose of processing:* We process this data to enable the performance of your work duties and the results and products of your work as owed under your employment contract.
- *Use justification: Performance of your employment contract (Article 6(1)(b), and § 26 (1) BDSG)*
- *Storage duration:* We store your data until the end of your employment. We might store some of the data for a longer time if it is needed for the fulfilment of a legal obligation or defence against legal claims. To the extent that your personal data form part of the work product we do not delete it.

2.4 Payroll

- *Types of data:* Tax number, social security number, tax class, health insurance, existence of secondary activities, children name and birthdate, work permit, payment data (IBAN / Sort Code), religious affiliation
- *Purpose of processing:* We process your data to facilitate payment of your salary as well as other payments owed (e.g. Reimbursements)
- *Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR, Fulfilling a legal obligation (Article 6(1)(c) GDPR)
- *Storage duration:* We will retain accounting data in accordance with the commercial and tax law storage obligations of six or ten years.

2.5 Work time management

- *Types of data:* Name, sick note, hours worked (Sheet), potential causes for illness (only when risk of infections for other employees)
- *Purpose of processing:* We process your data to manage your worktime. For regular employees this means managing your regular leave times, your time spent working from abroad as well as your sick leave. This also includes managing absences company wide and communicating those to the relevant teams. For employees paid on an hourly bases we also process your data to calculate your salary.
- *Use justification:* Performance of your employment contract (Article 6(1)(b), 9(2)(b)
- *Storage duration:* We will retain your work time management data according to applicable legal retention obligations of 4-7 years for records of working hours and 7 years for sick leave data.

2.6 Employee retention management (office parties, offers, etc.)

- *Types of data:* Name, email address

- *Purpose of processing:* We process your data to plan and execute company events such as office parties, to provide you with special offers (e.g. Gym, company bike, etc.).
- *Use justification: Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR
- *Storage duration:* We store your data until the end of your employment.

2.7 Travel Management

- *Types of data:* Name, email, home address, passport data (passport no., date of issuance/ expiration, etc.)
- *Purpose of processing: We process your data to organize business trips on behalf of existing employees or travel to a job interview at Ada for applicants.*
- *Use justification:* Use justification: Performance of your employment contract (Article 6(1)(b) GDPR and § 26 (1) BDSG)
- *Storage duration:* Your data will be stored for the duration necessary to comply with legal and contractual requirements resulting from the trip.

2.8 Internal use of personal data

- *Types of data:* Name, email, photo (where applicable)
- *Purpose of processing:* We process your data to create to enable company-wide communication and interaction that is not strictly work related. The use of certain data might be subject to your consent (e.g. your photo).
- *Use justification:* Our legitimate interest (Article 6 (1)(f) GDPR to create a positive and enjoyable work environment for our employees as well as your consent (Article 6(1)(a) GDPR)
- *Storage duration:* We store your data until the end of your employment. We will delete data that we process based on your consent when you revoke it.

2.9 Use of personal data on website

- *Types of data:* Name, email, photo (where applicable)
- *Purpose of processing:* We process your data to present our work and our key personnel on our website and present relevant contact points. The use of certain data might be subject to your consent (e.g. your photo).
- *Use justification:* Our legitimate interest (Article 6 (1)(f) GDPR to present our work in useful manner and make ourselves available for being contacted as well as your consent (Article 6(1)(a) GDPR).

- *Storage duration:* We store your data until the end of your employment. We will delete data that we process based on your consent when you revoke it.

2.10 Enforcement of pandemic restrictions

- *Types of data:* Name, vaccination status (number and data of vaccination), antigen test result (where applicable)
- *Purpose of processing:* We process your data to comply with pandemic restrictions such managing access to the office applicable to employers. Depending on the applicable regulations and guidelines, we might be required to check your vaccination status or quick test results upon entry to the office or other work-related gatherings.
- *Use justification:* Performance of your employment contract (Article 6(1)(b) GDPR or fulfilling a legal obligation (Article 6(1)(c) GDPR).
- *Storage duration:* We do not store data on your vaccination status or test results unless you have given us consent to do so. In this case, we delete your data when you revoke your consent or when the legal test requirement does not longer apply.

3. Where do we store your personal data

The personal data that we collect from you is generally stored in the European Union on Cloud Servers of Amazon Web Services EMEA S.A.R.L. (“AWS”) with a business seat in Luxembourg and on the Cloud Servers of Google Commerce Limited ("GCL"), a company incorporated under the laws of Ireland, with its offices at Gordon House, Barrow Street, Dublin 4, Ireland. This data may, however, be processed by sub-processors operating outside of the European Economic Area (“EEA”), namely the USA, based on a data processing agreement.

4. Disclosure of your personal data

4.1 We use technical service providers to operate and maintain our Services, who act as our processors based on a data processing agreement. Where we use Service providers who process personal data on our behalf outside the EEA (or “**third countries**”) we do so with the appropriate safeguards for your data subject rights. For all our service providers we either rely on an applicable adequacy decision (for the US this is currently the EU-US Privacy Framework) or include the standard contractual clauses in our data processing agreements.

4.2 In addition, we do not transfer your personal data to third parties - with the exception, when applicable, of the purposes listed below

- *Use justification:* The legal basis for the transfer and processing of your personal data by the processor corresponds to the legal basis on which we, as data controller, rely (always in compliance with section 3 above).

4.3 If we sell or buy any business or assets, we may disclose your personal data to the prospective seller or buyer of such business or assets.

- *Use justification:* Legitimate interest (Article 6(1)(f) GDPR): to sell our business or assets / where required by applicable law: consent (Article 9(2)(a) GDPR): for the processing of special categories of data, i.e. your personal health data.

4.4 If we or, substantially, all of our assets are acquired by a third party, personal data about our users will be one of the transferred assets.

- *Use justification:* Legitimate interest (Article 6(1)(f) GDPR): to sell our company or assets / where required by applicable law: consent (Article 9(2)(a) GDPR): for the processing of special categories of data, i.e. your personal health data.

4.5 If we are required on the basis of EU law or the law of a Member State to disclose or share your personal data.

- *Use justification:* Legal obligation (Article 6(1)(c) GDPR).

5. How long do we retain your personal data

We will hold your personal data for as long as it is necessary or required by law or by any relevant regulatory body, and always in compliance with the data minimization principle. Specific storage periods for the respective processing activities are detailed in section 3 above.

If your personal data is used for more than one purpose, we will retain it until the purpose with the longest period expires, but we will stop using it for the purpose with the shorter period as soon as the shorter period expires (to comply with the purpose limitation principle). We restrict access to your personal data to the persons who need to use it for the relevant purpose(s), always in compliance with the integrity and confidentiality principle.

After the processing of your data is no longer necessary for the purposes outlined in section 3 we will securely and separately store some of your data in accordance with statutory retention obligations applicable to us and reasonable business needs.

The retention period for the majority of your data ends when your employment with Ada is terminated. However, this does not mean that your data will be deleted at this point. The deletion period will often be longer, e.g. we will keep your personnel file for 3 years after the end of your employment.

Please be aware, that Ada will not delete data that is considered to be an owed work results by you. This might extent to any creation attributable to you, your communication with other employees (emails, Slack messages, etc.), comments, presentations, photo/video recordings, etc.

6. Your data subject's rights

Under GDPR you have various rights in relation to your personal data (as listed below). All of these rights can be exercised by contacting us via our contact form, by selecting "Exercising My Data & Privacy Rights".

- **Right to withdraw consent**: Where the processing of your data relies on your prior consent, you have the right to withdraw such a consent at any time by notifying us via email at dpo@ada.com. By withdrawing your consent, the lawfulness of the processing based on consent up until the point of withdrawal will not be affected.
- **Right to object**: As a data subject, you have the right to object on grounds relating to your particular situation, at any time, to the processing of your personal data which is based on Article 6(1)(f) GDPR ("legitimate interest" as indicated above) including profiling based on those provisions. In the event of an objection relating to your particular situation, we will no longer process your personal data, unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.
- **Right to be informed**: As a data subject, you have a right to obtain access and information under the conditions provided in Article 15 GDPR. This means in particular that you have the right to obtain confirmation from us as to whether we are processing your personal data or not. If so, you also have the right to obtain access to the personal data and the information listed in Article 15(1) GDPR. This includes information regarding the purposes of the processing, the categories of personal data that are being processed, and the recipients or categories of recipients to whom the personal data have been or will be disclosed.
- **Right to erasure / 'Right to be forgotten'**: As a data subject, you have a right to erasure ("right to be forgotten") under the conditions provided in Article 17 GDPR. This means that you generally have the right to obtain from us the erasure of your personal data and we are obliged to erase

your personal data without undue delay when one of the reasons listed in Article 17(1) GDPR applies. You can do this by deleting your account, in the App, at any time. If we have made the personal data public and are obliged to erase it, we are also obliged, taking account of available technology and the cost of implementation, to take reasonable steps, including technical measures, to inform controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of those personal data (Article 17(2) of the GDPR. The right to erasure ("right to be forgotten") does not by exception apply if the processing is necessary for one of the reasons listed in Article 17(3) GDPR. This can be the case, for example, if the processing is necessary for compliance with a legal obligation or for the establishment, exercise or defense of legal claims (Article 17(3)(b) and (e) GDPR).

- **Right to restriction of processing**: As a data subject, you have a right to restriction of processing under the conditions provided in Article 18 GDPR. This means that you have the right to obtain from us the restriction of processing if one of the conditions provided in Article 18(1) GDPR applies. This can be the case, for example, if you contest the accuracy of the personal data. In such a case, the restriction of processing lasts for a period that enables us to verify the accuracy of the personal data (Article 18(1)(a) GDPR). Restriction means that stored personal data are marked with the goal of restricting their future processing (Article 4(3) GDPR).
- **Right to data portability**: As a data subject, you have a right to data portability under the conditions provided in Article 20 GDPR. This means that you generally have the right to receive your personal data with which you have provided us in a structured, commonly used and machine-readable format, and to transmit those data to another controller without hindrance from us where the processing is based on consent (pursuant to Article 6(1)(a) or Article 9(2)(a) GDPR or on a contract (pursuant to Article 6(1)(b) GDPR), and where the processing is carried out by automated means (Article 20(1) GDPR). In exercising your right to data portability, you also generally have the right to have your personal data transmitted directly from us to another controller where technically feasible (Article 20(2) GDPR).
- **Right to Rectification**: As a data subject, you have the right to rectification under the conditions provided in Article 16 GDPR. This means in particular that you have the right to receive from us, without undue delay, the rectification of inaccuracies in your personal data and completion of incomplete personal data.

- **Right to complain**: As a data subject, you have a right to lodge a complaint with a supervisory authority under the conditions provided in Article 77 GDPR. The supervisory authority responsible for us is Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; https://ico.org.uk/make-a-complaint/ .

7. Changes to this policy

Any changes we make to our Privacy Policy in the future will be posted on this page, and where appropriate, notified to you by email, or by any other available means. We therefore encourage you to review it from time to time to stay informed about the way we are processing your data.

Last updated: July 5th, 2024