Roles within the GDPR framework

Businesses can take on a number of roles within the framework of GDPR as defined by Article 4. This is how Traitly views those roles and their associated responsibilities:

Data Controller

The ‘data controller’ is the party that determines the purposes and means of the processing of personal data. Traitly serves as a Data Controller to the extent that Traitly discovers and engages candidates for the Customer from publicly-available data sources on the Web. The Customer also serves as a data controller in that they determine the purpose (recruiting the candidate) and the means (using Traitly) of processing the individual’s personal data once their data has been passed to it by Traitly.

Data Processor

Traitly also serves as a data processor, in that we process data on your behalf. We do not own the data in your Applicant Tracking System.

Traitly’s commitment to GDPR compliance and data privacy

Here is an overview of how Traitly meets the new regulatory requirements:

Data inventory

We reviewed and identified all the areas of Traitly where we collect and process customer data, validating with our own legal consultants our basis for collecting and processing personal data in compliance with our obligations as a data controller. We ensured that we apply the appropriate security and privacy safeguards across our infrastructure and software ecosystem, as outlined in our Data Security and Processing Agreement document.

Individual data subjects' rights – data access, portability and deletion

The GDPR gives data subjects the right to request access to, correction of, or deletion of their personal data in certain circumstances. Where acting as your processor, your assigned Traitly account coordinator complies with this request by deleting the candidates' data from your Traitly account. We store personal data until your account is deleted, after which we dispose of all data in accordance with our Terms & Conditions and Data Security and Processing Agreement.

Risk assessment (Data Protection Impact Assessments)

A requirement of GDPR is having a managed data protection impact assessment (DPIA) process. A DPIA process is a way to help identify and minimise the data protection risks of a project by ensuring that proper security and privacy due diligence is conducted when choosing tools and making implementation decisions. Traitly has always developed our services with the goal of mitigating any risk to data privacy or security so we have and will continue to meet these obligations.

In order to ensure that your handling of data is compliant with GDPR, you should verify that your internal data processes and all of your data vendors meet the following criteria:

Lawfulness of processing

Articles 6 and 7 require that data controllers ensure that they have a lawful basis for processing personal data from a data subject within the EU. This could be through the receipt of consent from the data subject or processing based on the controller's legitimate interests. Traitly believes that because (1) you have a legitimate interest in contacting the candidate regarding a role at your company, (2) you are not offering sales or services, and (3) there is no alternative method to contacting them that would not involve processing their personal information, your use of Traitly to reach out to potential candidates is covered by the legitimate interest provision. Reaching out to someone regarding a job opportunity is also to their benefit and supports their right to freedom of employment.

Providing information to end users (Article 15)

Under the GDPR, the data subject has the right to obtain from any data controller certain information about how their personal data is processed and by whom. Your

assigned Traitly recruitment coordinator will be responsible for fulfilling these requests.

Support for data access and deletion requests (Articles 16-23)

The GDPR gives data subjects the right to request access to, correction of, or deletion of their personal data in certain circumstances. Your dedicated Traitly recruitment coordinator is responsible for complying with this request by deleting the candidates' data from your Traitly account. We do not delete the metadata associated with an individual during this process so that we can keep a record of their request to be deleted. We believe this fulfills the requirements of the GDPR provision while meeting the expected behavior of the individual. If we also deleted the metadata associated with their data, you could potentially source and contact them again in the future as we would have no record of the deletion request. For individuals who want to access the personal data you keep on them, all of the relevant data can be exported from your Traitly account in a computer-readable CSV format for any candidate in your projects. Traitly will respond to these data requests by providing all of the information for any individual in a computer-readable CSV format per the GDPR requirements.

Data protection by design and by default (Article 25)

Under the GDPR, controllers must consider the principles of data minimization and privacy by design, and must consider minimizing their data collection to the amount necessary to accomplish a given task. Traitly believes we are effectively helping you meet this obligation by limiting the data collected for a candidate to only the information relevant to their suitability for your roles and that which you would need to effectively engage with them. If your interpretation of this article also includes an expectation that data should be deleted within a specific time period, we can support those requests. However, we believe that candidates would reasonably expect you to remember your interaction with them about a potential job opportunity, and thus retaining records of your interaction is appropriate, even after several years.

Records of processing activities (Article 30)

Under the GDPR, processors are required to keep records of their processing activities, including those activities conducted by their subprocessors. Traitly

maintains proper processing logs to comply with this provision and can supply them upon request.

Data breach notifications (Articles 33-34)

Under the GDPR, controllers and processors are required to provide notifications of data breaches without undue delay. Our policies and timeframes for breach notifications based on severity can be found in our Data Security and Processing Agreement.

Security (Articles 40-43)

Security is a key principle under the GDPR. Controllers should ensure that their personal data is processed by vendors who have implemented appropriate security standards, and Traitly has implemented what we believe to be an industry-leading security and compliance program for our product infrastructure.

Cross-border data transfers (Articles 44-50)

When transferring data outside the EU, controllers should ensure that their personal data is protected by the legal requirements substantially similar to those set by the EU.