For copies of any of the documents referenced in these terms, please reach out to amelialegal@soundhound.com

GDPR Product Readiness

Last Modified April 13, 2018

Our Lawyers Are Making Us Say This: This is neither legal advice for your company in complying with GDPR/other data privacy laws nor a magnum opus on EU/EEA data privacy. What we are providing is background information to help you better understand how Amelia has addressed some important legal points. This legal content is not the same as legal advice, where an admitted attorney applies the law to your specific circumstances, and you must consult an attorney if you'd like advice on your interpretation of this information or its accuracy. In summary, you may not rely on this microsite as legal advice, nor as a recommendation of any particular legal understanding.

Regardless of your company's size, everyone's got the General Data Protection Regulation (GDPR) on their mind. The GDPR is focused on enhancing protection of EU citizens' personal data and increasing the obligations of organizations to deal with that data in transparent and secure ways. The GDPR applies not only to EU-based businesses, but also to any business that controls or processes data of EU citizens.

At Amelia, our entire organization is working hard to ensure that our own operations GDPR-compliant. But equally important to us is helping you, our partners and customers, by ensuring that Amelia products and services are set up for GDPR compliance. In full transparency, while our existing products can be used GDPR-compliant manner, we've set out to make it far easier and convenient to ensure compliance without extensive workaround and delays.

Between now and May 25th (and beyond), we are fully committed to enhancing Amelia products and services to enable easier compliance with the GDPR.

Amelia Product and Service Readiness

For many companies – including Amelia – GDPR compliance is stressful and work-heavy. We've recognized that this is important, however, in order to provide better, more secure, more transparent experiences for our customers (and their customers).

Below is a detailed list of the features we're building to help you be compliant. A quick note on timelines: we've already started (and in many cases, finished!) building many of these new features, and we'll continue to develop our products and features through 25 May 2018 and beyond. Our planned timeline is to have every feature on this list completed by May 25, 2018.

But first, a quick primer on the legalese associated with the GDPR (and you can find out more definitions on our FAQs and Glossary page):

- Data Subject: The individual human being whose sharing information with you (for these examples, we're calling him "Edwin").
- Data Controller: Your company, as the customer of Amelia (for these examples, we'll call your company "ABCcorp").
- Data Processor: In these examples, Amelia, to the extent that we are processing Edwin's data on behalf of ABCcorp. Please keep in mind that Amelia will only be the Data Processor if we're actually processing the data in an Amelia-hosted environment; if you (that is, ABCcorp) has an on-premise implementation, the functionality will be available but Amelia will not be the Data Processor.

Lawful basis of processing

What This Means: There needs to be a legal reason to use Edwin's personal data, whether consent with notice (you told Edwin what he was opting into), performance of a contract (for example, Edwin is ABCcorp's customer and ABCcorp wants to invoice him),

or what the GDPR calls “legitimate interest” (e.g. Edwin’s a customer, and you want to send her products related to what she currently has).

What Amelia is Doing: Amelia relies on ABCcorp’s collection of lawful basis, since we don’t have direct contact with your customers. If you have worked with us to set up the proper integrations, a change in lawful basis (such as Edwin withdrawing consent) should be “passed along” and implemented automatically.

Deletion

What This Means: Edwin has the right to request that you delete all the personal data you have about him. The GDPR requires the permanent removal of Edwin’s information from your databases. In many cases, you’ll need to respond to his request within 30 days. The right to deletion is not absolute, and can depend on the context of the request, so it doesn’t always apply.

What Amelia is Doing: You will be able to perform a GDPR-compliant permanent delete in the software.

Access / Portability / Modification

What This Means: Just as she can request that you delete her data, Edwin can request access to the personal data you have about him. Personal data is anything identifiable, like his name and email address. If Edwin requests access, you (as the controller) need to provide a copy of the data, in some cases in machine-readable format (e.g. CSV or XLS).

If Edwin asks you to modify his personal data, updates to that record will “flow down” if the proper integrations are configured.

What Amelia is Doing: You’ll be able grant any access/portability request by easily exporting Edwin’s record(s) into a machine-readable format. Other information (for example, an AMELIA chat log) will be available to be exported as well.

Security Measures

What This Means: The GDPR requires a slew of data protection safeguards, from encryption at rest and in transit to access controls to data pseudonymization and anonymization.

What Amelia is Doing: As part of Amelia's approach to the GDPR, we're reviewing and enhancing security controls across the board. In addition to industry standard practices around encryption, Amelia's infrastructure teams are also improving our systems for authentication, authorization, and auditing at a massive scale to better protect our customer's data. We will provide additional details on these security measures as they are implemented here.

Employee Training

What this Means: Article 39 of the GDPR requires employees involved in "processing operations" be trained in privacy and security practices to do their jobs.

What Amelia is Doing: Amelia's representatives discuss privacy and security practices with all new employees during onboarding. Amelia then requires all employees take an additional online information security and privacy training course. For those employees who might need to access Edwin's data (in the context of their role) to support or deliver our products and services will also participate in further education, covering topics such as confidentiality and responsibilities of a processor. All Amelia employees also have yearly security and privacy training sessions. In addition, Amelia's security and privacy employees work with our R&D teams to ensure privacy and security by design.

If you're already an Amelia customer or partner, please contact your account manager if you have any further questions, comments, or suggestions.