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

Key Changes Under the GDPR

Last Modified October 18, 2024

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.

The Key and Most Important Changes Under the GDPR

Although the 1995 Data Protection Directive (DPD) was a substantial and important privacy regulation, the GDPR implements quite a few changes to better protect the personal information of individuals. These can be viewed in four major categories – (i) Individual Rights, (ii) Internal Procedures, (iii) Supervisory Authorities, and (iv) Scope, Accountability, and Penalties.

We've gathered the key changes here with a brief explanation of each major and important change. Again, keep in mind that this isn't legal advice – so you should check with your own legal advisors if you have further questions.

Individual Rights

Consent

Whenever a data subject is about to submit their personal information the data controller (usually a company) must make sure the data subject has given their consent. The GDPR sets a higher standard for disclosures when obtaining consent, as it needs to be “freely given, specific, informed and unambiguous,” with controllers using “clear and plain” legal language that is “clearly distinguishable from other matters”. Controllers will also be required to provide evidence that their processes are compliant and followed in each case. Under the DPD, consent could be inferred from an action or inaction in circumstances where the action or inaction clearly signified consent. Thus, the Directive left open the possibility of “opt-out” mechanism. However, under the GDPR, the data subject must signal agreement by "a statement or a clear affirmative action."

Essentially, your customer cannot be forced into consent or be unaware that they are consenting to processing of their personal data. They must also know exactly what they are consenting to and they must be informed in advance of their right to withdraw that consent. Obtaining consent requires a positive indication of agreement – it cannot be inferred from silence, pre-ticked boxes, or inactivity. This means that informing the user during the opt-in is becoming more important in the future.

Rights for Individuals

The regulation also has rights for data subjects: a "*right to be forgotten*" that requires controllers to alert downstream recipients of deletion requests and a "*right to data portability*" that allows data subjects to demand a copy of their data in a common format. These two rights will now make it easier for users to request that any information stored should be deleted or that information that has been collected should be shared with them. We do want our customers to keep in mind that when you purchase Amelia products or services, Amelia isn’t a “data controller” – we’re a data processor.

Access Requests

Data subjects always had a right to request access to their data - the GDPR enhances these rights. In most cases, you will not be able to charge for processing an access request, unless you can demonstrate that the cost will be excessive. The timescale for processing an access request will also drop to a 30-day period. In certain cases, organizations may refuse to grant an access request, for example where the request is deemed manifestly unfounded or excessive. However, organizations will need to have clear refusal policies and procedures in place and demonstrate why the request meets these criteria.

Internal Business Procedures

Privacy by Design and DPIA

There are several new principles for entities that handle personal data, including a requirement to build in data privacy *"by design"* when developing new systems and an obligation to perform a Data Privacy Impact Assessment (DPIA) when processing using *"new technologies"* or in risky ways. A DPIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals so that potential privacy issues can be identified before they arise, giving the organization time to come up with a way to mitigate them before the project is underway.

Data Privacy Officer

On the security side, the GDPR will require many businesses to have a Data Privacy Officer (DPO) to help oversee their compliance efforts. Organizations requiring DPOs include public authorities, organizations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organizations who process what is currently known as sensitive personal data on a large scale. However, keep in mind that *any* organization can appoint a DPO, even if none of those requirements apply.

While the GDPR currently preserves the DPD's approved methods for ensuring *"adequacy"* when transferring personal data to third countries, DPOs will also be helpful in overseeing a controller's relationships with vendors who process and store personal data, helping to review vendors' security practices and inform vendors of data subject requests.

Contracts & Privacy Documentation

Since the GDPR is all about transparency and fairness, Controllers and Processors will need to review their Privacy Notices, Privacy Statements, and any internal data policies to ensure they meet the requirements under the GDPR. If a Controller engages third party vendors to process the personal data under their control, they will need to ensure their contracts with those Processors are updated to include the new, mandatory Processor provisions set out in Article 28 of the Regulation.

Supervisory Authorities

One-Stop Shop

One item in the GDPR should serve to make the lives of these DPOs easier: the GDPR's new *"one stop shop"* provision, under which organizations with offices in multiple EU countries will have a *"lead supervisory authority"* to act as a central point of enforcement so they don't struggle with inconsistent directions from multiple supervisory authorities.

Reporting Breaches

The GDPR contains a new requirement that controllers must notify their country's supervisory authority of a personal data breach within 72 hours of learning of it, unless the data was anonymized or encrypted. Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned.

Scope, Accountability, and Penalties

Scope

While the current legislation, the 1995 EU Data Protection Directive, governs entities within the EU, the territorial scope of the GDPR is far wider, in that it will also apply to non-EU businesses who market their products to people in the EU or who monitor the behavior of people in the EU. In other words, even if you're based outside of the EU but you control or process the data of EU citizens, the GDPR will apply to you.

Accountability

This new concept will require Controllers and Processors to be able to demonstrate their compliance with the GDPR to their local supervisory authority. Processes should be recorded, implemented, and reviewed on a regular basis. Staff should be trained, and appropriate technical and organizational measures should be taken to ensure and demonstrate compliance.

Severe Penalties

The importance of the GDPR's new provisions is underscored by the new penalties it imposes for violations. Depending on the type of violation in question, controllers and processors who mishandle personal data or otherwise violate data subjects' rights could incur fines of up to €20 million or 4% of their global annual revenue (whichever is greater).

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