GDPR Key Facts

What GDPR means for you?

The General Data Protection Regulation ("GDPR") is the privacy law that went into effect in the European Union in May 25, 2018. GDPR has been years in the making and builds on the principles of the 1995 data protection directive from 1995: a time when Netscape Navigator was the browser to use, 3.5" floppy disks were the only way to save data, and kilobits is how speed was measured. Technology has changed significantly as well as the role of data and data-sharing as it is used in business, so it was time for an update. This material highlights how you can rest assure that the data you share with IntelePeer, whether of your employees, customers, or users, will enjoy the key protections of the GDPR.

What are the key protections of the GDPR?

Basically, the GDPR gives individuals more power to control their personal data that companies collect, use, and share about those individuals, which requires more transparency from the companies about their use and security of the data. The GDPR is applicable to any organization established in the EU and to any organization, regardless of where the organization is located, that processes the personal data of EU individuals when offering them goods or services or when monitoring or tracking their activities., Specifically, the GDPR ensures that the personal data of EU individuals is:

- Processed fairly, lawfully and transparently
- Collected and processed for specific reasons and stored for specific periods of time, and not used for reasons beyond its original purpose
- Only the data necessary for the purpose it is intended is collected, and not more
- Accurate and that reasonable steps are taken to ensure it remains accurate
- Kept in a form that allows individuals to be identified only as long as is necessary
- Secured and protected from unlawful access, accidental loss or damage
- Subject to the exercise of individuals' rights to access, correct, object, delete and port such personal data

GDPR requires organizations, like IntelePeer and our customers, who are collecting, using and storing personal data, to expressly define the lawful purpose that the organization will use that personal data, pursuant to the above six principles. For more detail on how IntelePeer uses and protects the personal data you share with us as your service provider, please reference the IntelePeer Privacy Policy.

What is the "personal data" protected by GDPR?

The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person", "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Although pieces of information alone may not be considered "personal data", when that information is collected or used in combination with other information, the information could be used to reasonably determine someone's identify—making the information "personal data". In order to offer innovative and competitive services, IntelePeer may utilize various types of personal data, including for example names, emails, telephone numbers, website cookies, communications records and associated metadata, related to the employees, users, and customers of our customers. For more detail on what personal data IntelePeer uses and how IntelePeer manages such personal data, please reference the IntelePeer Privacy Policy.

What are some of the bases for lawful processing personal data?

The bases for lawful processing will depend on the type of processing that you or your sub-processors are doing. The two most common bases for lawfully processing personal data are:

- Individuals have given specific, informed and unambiguous consent, in a clear, affirmative action, to the processing of their personal data for one or more specific purposes. (Please note that those individuals may refuse or withdraw such consent without penalty, though refusal or withdrawal of consent may result in limited functionality of the underlying services, systems or websites.)
- Processing is necessary for the performance of a contract to which the individual is a party, or in order to take steps at the request of the individual prior to entering into a contract.

Other types of lawful processing can be found in Article 6 of the GDPR.

What is the difference between a data processor and a data controller?

A Controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the Processor is an entity which processes personal data on behalf of, and at the direction of, the controller. Specifically, the GDPR defines:

- Controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"; and
- Processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

The GDPR establishes different obligations for Controllers and Processors, so it is important to understand whether who is the Controller and who is the Processor for the different types of personal data processed by you, your customers and your Processors. For personal data collected directly from an individual, such as a user of our website, IntelePeer acts as the Controller of such data. When our customers share information about their customers or employees with IntelePeer for use to provide our services, IntelePeer acts as the Processor.

Does personal data collected by IntelePeer remain in the EU?

For our customers based in the EU, any personal data shared with IntelePeer for use of our services on the CPaaS platform will remain inside the EU, unless such personal data is contained in a messaging or voice communication made via the CPaaS platform and sent to a country outside of the EU. Any personal data of customers outside of the EU from their use of CPaaS services may be served out of our systems and platforms in the US. All personal data used by IntelePeer for the administrative aspects of supporting all of our customers' accounts, such as account information, accounts receivable information and support tickets, will be maintained in the US, and will be transferred pursuant to the EU-US Privacy Shield obtained by IntelePeer.

How does IntelePeer secure the personal data it collects, transmits and stores?

Securing personal data is a top priority for IntelePeer. IntelePeer employs current industry standards and state-of-the-art technologies to secure the personal data collected, transmitted and stored as part of using its services, portals or website, depending on the sensitivity and risks associated with the particular personal data. Such measures may include, as appropriate: (a) the pseudonymization, encryption and minimization of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; or (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. For more information about the security measures employed by IntelePeer, please reference our technical and organizational security measures documentation found in our IntelePeer Privacy Policy. For any questions, concerns or complaints related to this Policy, please contact IntelePeer at mailto:infosecurity@intelepeer.com.