Align Technology ("Align") – Customer FAQs about Data Protection

Updated March 6, 2018

This sheet contains information about data protection, privacy, and, in particular, how Align complies with the European Union's General Data Protection Regulation (the "**GDPR**"). It also aims to better inform you, the doctor, regarding the patient data you provide to Align.

In order for Align to manufacture Invisalign® aligners, its customers need to provide Align with certain patient data. This data includes the patient's name, gender, date of birth, as well as the moulds or scans of the patient's dentition and other dental records. Align's dental technicians work closely with its customers and during these exchanges further patient data may be transferred to Align. All patient data provided to Align ("**Patient Data**") is considered personal data and the EU, and many countries outside the EU, have laws which protect the collection, use, storage, and transfer of the personal data of their citizens.

Align has taken steps so that its customers can confidently transfer Patient Data to Align, knowing that both the customer and Align are in compliance with the applicable laws in the customer's country.

When does the GDPR go into effect?

The GDPR will take effect on May 25, 2018. Unlike the current Data Protection Directive which is brought into effect through legislation in each EU member state, the GDPR will automatically becomes law without the need for local legislation. However, each member state will have its own supplementary legislation which clarifies certain aspects of the GDPR or provides additional rules to complement the GDPR.

What are the relevant roles of Align, the patient, and the doctor under GDPR?

Align's relationship with doctors and patients remains unchanged under the GDPR. When doctors transmit Patient Data to Align for treatment purposes they are the Controller, Align is the Processor, and the patient is the Data Subject.

Align sometimes acts as a controller in its relationship with patients and doctors, for example when Align collects information about doctors for the purposes of marketing, sales and managing the relationship with the doctor. Align is sometimes a controller of data about patients and future patients, for example when it markets the services of Align and doctors on its website and in other marketing materials, and when patients register their aligners with Align.

To whom does the GDPR apply?

The GDPR applies to persons or organizations processing personal data of EU data subjects, which includes Align and doctors.

What is Align doing to prepare for the GDPR?

Align has been working on preparing for the GDPR since late 2016 and is well advanced in its preparations. Some of the things Align has been doing to prepare include:

- Appointing a data protection officer to continue the development of Align's commitment to data protection.
- Amending its contracts with vendors and doctors to ensure the terms comply with the GDPR.
- Carrying out Data Protection Impact Assessments to identify and minimise risks to Patient Data.
- Ensuring its privacy policies and notices clearly explain Align's commitment to the GDPR and the rights which individuals have with respect to their data.

How can I be sure that my Patient Data is adequately protected after the GDPR goes into effect?

Align's Pricing Terms & Conditions have been amended so that cases submitted after May 25, 2018 will be subject to the new terms developed for use with doctors reflecting the requirements of the GDPR.

Cases that have already been submitted will of course be protected to the same standards as new cases going forward.

Am I allowed to send my patients' records to Align?

Yes. When you obtain a patient's consent to treatment using the Align Patient Consent Form, the form also contains consent to process Patient Data for the purposes of that treatment. It also provides notice to patients according to the GDPR requirements that Align may process the Patient Data.

What wording should I use to obtain consent from patients?

Because dental records are sensitive health data, you need to be careful about the words you use on your consent forms. Align has provided a template Informed Consent Agreement that is available on the Invisalign Doctor Site ("**IDS**").

What happens to the records I send to Align?

Patient Data is sent to Align's treatment-planning specialists outside of the European Union for analysis. Data is then transferred to Align subsidiaries around the world, so that dental aligners can be manufactured and our dental technicians can work with you as required when reviewing the ClinCheck® treatment plan. Other Align subsidiaries can also see this data for regulatory, quality control, and customer service reasons.

Align does not retain Patient Data in its systems longer than necessary and only uses personal data for the purposes mentioned in our privacy notices.

What data protection standards does Align follow?

The Invisalign Pricing Terms and Conditions or the iTero® Purchase Terms and Conditions you accept each time you place an order with Align include substantial data protection provisions (which are now in accordance with GDPR requirements). These provisions include commitments from Align to comply with the applicable local data privacy laws of the countries where the data is collected. The permission to collect the data locally relies on the consent of the patient, which the doctor has to collect.

Moreover, Align has committed itself to comply with an internal set of rules on how Align is permitted to process and transfer personal data. These rules have been agreed upon and accepted by all the European data protection authorities and endorsed by the European Commission. This is intended to ensure that the EU level of data protection will be followed throughout the Align group, and is considered the gold standard of compliance globally. These are known as "Binding Corporate Rules" or BCRs and have been in place for Align since 2014.

How do I know the data I'm transferring to Align is secure?

Align has put in place appropriate technical and organisational security measures to protect Patient Data. Under its BCRs, Align must comply with the security obligations of the EU country from which you are transferring the data as specified in the Invisalign Pricing Terms and Conditions or the iTero Purchase Terms and Conditions. Align subsidiaries to which we transfer data have adopted equivalent security measures in order to comply with the GDPR.

What are Align's obligations in the event of a data breach?

Align will notify the relevant Customer without undue delay if Align becomes aware of a verified Data Breach and will keep the Customer informed of any related developments. Align will take all reasonable steps to mitigate or negate the effects of any such data breach. However, as the controller of the Patient Data it is the doctor's responsibility to inform the relevant regulator. Align will provide reasonable assistance to the Doctor to do this.

What is the situation with patient transfers and compliance with data privacy?

There are situations in which a patient may ask to be transferred to another provider. Align will always try to obtain the written consent of the doctor from whom the patient wishes to be transferred.

However, where that is not possible and for whatever reason, as long as Align has a signed written consent from the new doctor, Align will respect the wishes of any patient who has provided a signed written consent to the transfer.

By accepting the Invisalign Pricing Terms and Conditions when you order you agree to Align transferring the relevant Patient Data to a new doctor in these circumstances and without you providing a separate written consent to the individual transfer.

What about third parties who work with Align?

When Align contracts with a third party that in any way interacts with Patient Data, Align first requires that these third parties pass a security and risk assessment to ensure they uphold the same standards as Align with respect to personal data. In addition, GDPR requires that these companies are contractually obligated to implement and uphold equivalent security measures to protect Patient Data. Align also maintains a list of the types of third parties who might be engaged by Align at http://www.aligntech.com/privacy_policy.

Does Align use Safe Harbor or Privacy Shield?

You may have heard that the main regime to transfer data from the EU to the US, known as Safe Harbor, was declared invalid in 2015. This has now been replaced by the more robust Privacy Shield. However, Binding Corporate Rules (BCRs) are considered the gold standard by the EU and therefore Align will continue to use these to ensure compliance with the GDPR.

What if one of my patients asks for their dental records?

Any patient has a right to see all data you hold about them. This is called a "subject access request". If a patient makes a subject access request directly to Align, we will pass the request on to you as soon as practicable and, where Align holds the data requested, Align will assist you to provide the patient with the data requested.

Can patients ask for anything else?

As well as the right to access data you hold about them, patients may also have the right under GDPR to have inaccurate or incomplete data rectified, have their data deleted or to ask that you stop processing their data. Patients can also ask you to transfer data they have provided to you to another doctor. If a patient wishes to exercise any of their rights in relation to their Patient Data, we will inform you of such a request and provide you with reasonable assistance in honouring those requests. Note that you are not always required to carry out such requests by patients as GDPR provides that you only need to comply in certain situations.

What about the records Align holds about me?

Align also collects your personal data in order to promote Align products, handle orders, and respond to enquiries. These data are protected by the same security measures and are also covered by our BCRs. Our updated Customer Privacy Policy contains details of how Align processes your personal data and the rights that you have under GDPR with respect to it.

Who at Align should I contact with concerns regarding the GDPR or Privacy?

You may direct all questions regarding the GDPR and Privacy to Align's Data Protection Officer at Privacy@aligntech.com.

What do I need to do to ensure that I comply with data privacy laws when working with Align?

In order to ensure that YOU are compliant with data privacy laws in your dealings with Align you must ALWAYS:

1. obtain a valid patient consent before sending any Patient Data and provide notice to Patients about how their data is processed;

2. keep your login details secret and secure, and do not share them with any person, particularly if they are not part of the same dental practice; and

3. log-out of any systems on which you have been accessing Align's systems when not in use.