Align Technology

Data Protection Binding Corporate Rules Processor Policy

Change Log	
9 June 2014	Original.
23 April 2019	Updated due to General Data Protection Regulation.
19 October 2022	Updated due to legal developments in relation to international transfers restrictions, and other minor edits in Rule 6D and Appendix 2. Amendments linked to appointment of external DPO and update of the privacy training titles. Amendments with regards to certain processes and updates to align to the standard wording of Align's internal policies.
29 November 2023	Updated to account for new BCR lead and Liable BCR Member.
18 July 2025	Updated to remove controller relevant provisions from the Appendices.
9 October 2025	No substantive changes. Minor editorial refinements to ensure clarity and consistency.
July 2026	Updated to incorporate feedback from supervisory authority. Update of entity list.

© 2023 Align Technology, Inc. All rights reserved.

Contents

INTRODUCTION TO THIS POLICY **3**

PART I: BACKGROUND AND ACTIONS **4**

PART II: PROCESSOR OBLIGATIONS **6**

PART III: APPENDICES **16**

© 2023 Align Technology, Inc. All rights reserved.

INTRODUCTION TO THIS POLICY

This Data Protection Binding Corporate Rules Processor Policy ("**Policy**" or "**Processor Policy**") establishes Align's approach to the protection and management of personal information globally by Align group members, listed at www.aligntech.com ("**Group Members**"), when collecting and using that information on behalf of a third party.

Scope of this Policy

This Policy applies when we process personal information as a processor and transfer personal information between Group Members (including onward transfer to other BCR members outside of the EEA) as described in Appendix 8. The standards described in the Processor Policy are worldwide standards that apply to all Group Members when processing personal information as a processor. As such, this Policy applies regardless of the origin of the personal information that we process, the country in which we process personal information, or the country in which a Group Member is established.

Our collective responsibility to comply with this Processor Policy

This Policy applies to all personal information collected and used as part of the regular business activities of Align, both manually and by automated means, in the course of providing services to a third party controller (referred to as the "**Customer**" in this Policy) including personal information relating to patients that we process on behalf of physicians.

Group Members and their staff will comply with and respect this Policy when collecting and using personal information in their capacity as service providers, irrespective of the country in which they are located.

This Policy does not replace any specific data protection requirements that might apply to a business area or function.

Responsibility towards the Customer

When Align processes personal information as a processor, the Customer on whose behalf Align processes personal information will have responsibility for complying with the applicable data protection laws that apply to it. As a consequence, the Customer will pass certain data protection obligations on to Align in its contract appointing Align as its processor. If Align fails to comply with the terms of its processor appointment, this may put the Customer in breach of its applicable data protection laws and Customer may initiate proceedings against Align for breach of contract, resulting in the payment of compensation or other judicial remedies.

A Customer may enforce this Processor Policy against any Group Member that is in breach of it. Where a non-European Group Member (or a non-European third-party processor appointed by a Group Member) processes personal information for which the Customer is a controller in breach of this Processor Policy, that Customer may enforce the Processor Policy against Invisalign Spain, S.A. In such event, Invisalign Spain, S.A. will be responsible for demonstrating that such Group Member (or third-party processor) is not responsible for the breach, or that no such breach took place.

When a Customer transfers personal information to a Group Member for processing in accordance with this Processor Policy, a copy of this Policy shall be incorporated into the contract with that Customer.

Management commitment and consequences of non-compliance

Align's management is fully committed to ensuring that all Group Members and their staff comply with this Policy at all times. Non-compliance may cause Align to be subject to sanctions imposed by competent data protection authorities and courts, and may cause harm or distress to individuals whose personal information has not been protected in accordance with the standards described in this Policy.

© 2023 Align Technology, Inc. All rights reserved.

In recognition of the gravity of these risks, staff members who do not comply with this Policy will be subject to disciplinary action, up to and including dismissal.

Where will this Processor Policy be made available?

This Policy will be published on the website accessible at www.aligntech.com.

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

Data protection law gives people the right to control how their "**personal information**"[1] is used. Under data protection law, when an organisation collects, uses or transfers personal information for its own purposes, that organisation is deemed to be a *controller* of that information and is therefore primarily responsible for meeting the legal requirements.

When, on the other hand, an organisation collects and uses information on behalf of a third party (for example, to provide a service), that organisation is deemed to be a *processor* of the information and the third party will be primarily responsible for meeting the legal requirements.

HOW DOES DATA PROTECTION LAW AFFECT ALIGN INTERNATIONALLY?

Data protection law does not allow the transfer of personal information to countries outside of Europe[2] that do not ensure an adequate level of data protection. Some of the countries in which Align operates are not regarded by European data protection authorities as providing an adequate level of protection of individuals' data privacy rights.

When Align acts as a processor, Align's Customers retain the responsibility to comply with European data protection law.

In practical terms, this means that those acting as controllers in Europe will pass certain data protection obligations on to any processor which collects and uses personal information outside of Europe on their behalf in order to overcome the legal restrictions on international data transfers.

If Align fails to comply with the contractual data protection obligations its Customers pass on to it, its Customers may be in breach of applicable data protection law and Align may face a claim for breach of contract which may result in the payment of compensation or other judicial remedies. If a Customer demonstrates that it has suffered damage that is likely to have occurred because of a breach of this Policy, Align will bear the burden of proof to show that its non-European Group Member or non-European sub-processor was not responsible for the breach, or that no such breach took place.

WHAT IS ALIGN DOING ABOUT IT?

The purpose of this Policy is to set out a framework to satisfy the standards contained in European data protection law and, as a result, provide an adequate level of protection for all personal information transferred to Group Members in a third country , either where the personal information is collected by a Customer in Europe as a controller or where the personal information is collected by Align in Europe as a processor.

Although it will be for each of Align's Customers to decide whether the commitments made by Align in this Policy provide adequate safeguards for the personal information transferred to Align under the terms of its contract with Align, Align will apply the Rules (defined herein) contained in this Policy whenever it acts as a processor. As such, where Align's Customers rely upon this Policy as providing adequate safeguards, an

[1] Personal information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in the General Data Protection Regulation 2016/679.
[2] For the purposes of this Policy, reference to Europe means the EEA and Switzerland.

© 2023 Align Technology, Inc. All rights reserved.

obligation to comply with the Policy will be included in Align's contracts with its Customers and a copy of the Policy will be incorporated into such contracts.

This Policy applies to all Group Members and their staff worldwide and requires that Group Members who collect, use or transfer personal information to provide services to a third party as a processor will comply with the Rules set out in **Part II** of this Policy ("**Rules**") together with the policies and procedures set out in the appendices in **Part III** of this Policy.

For completeness, Group Members will comply with the Data Protection Binding Corporate Rules Controller Policy when they collect, use and transfer personal information as a controller. Some Group Members may act as both a controller and a processor and will therefore comply with this Policy and also the Data Protection Binding Corporate Rules Controller Policy as appropriate.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues you can contact Align's Privacy Office at the address below who will either deal with the matter or forward it to the appropriate person or department within Align.

Attention: **Privacy Office**

Email: **Privacy@aligntech.com**

Address: **Align Technology Switzerland GmbH**

Suurstoffi 22

6343 Rotkreuz

Switzerland

Align has appointed an external Data Protection Officer. Please use the contact details outlined above to contact Align's Data Protection Officer. Align's Data Protection Officer will become involved in data protection compliance matters, including in relation to the compliance with this Policy.

The Privacy Office is responsible for ensuring that changes to this Policy are notified to the Group Members and to individuals whose personal information is collected and used by Align.

If you are unhappy about the way in which Align has used your personal information, Align has a separate complaint handling procedure which is set out in Part III, Appendix 4.

IMPORTANT TERMS USED IN THIS POLICY

For the purposes of this Processor Policy:

- the term "applicable data protection laws" means the data protection laws in force in the territory from which a Group Member initially transfers personal information under this Controller Policy. Where a European Group Member transfers personal information under this Controller Policy to a non-European Group Member, the term applicable data protection laws shall include the European data protection laws applicable to that European Group Member (including the GDPR);
- the term "competent supervisory authority" means the supervisory data protection authority that is competent for the exporter of personal information;
- the term "EEA" means EU member states and Iceland, Liechtenstein and Norway.

- the term "exporter" means a Group Member who processes personal information subject to the GDPR as a controller or a processor on behalf of another Group Member, and transfers this personal

© 2023 Align Technology, Inc. All rights reserved.

information to another Group Member outside Europe (the importer) for further processing;

- the term "GDPR" means the EU General Data Protection Regulation 2016/679;
- the term "GDPR protected personal information" means personal information which processing is subject to European data protection laws;
- the term "importer" means a Group Member outside Europe who receives personal information from the exporter with a view to further processing this personal information as a controller or processor;
- the term "Lead Supervisory Authority" means the Spanish Data Protection Commissioner, or another supervisory authority appointed as the lead supervisory authority in the future;
- the terms "member state" means EEA members.
- the term "processing" means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- the term "special categories of data" means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about an individual's criminal offences or convictions as well as any other information deemed sensitive under applicable data protection laws; and the term "staff" refers to all employees, new hires, individual contractors and consultants, and temporary staff engaged by any Group Member;
- the term "third country" shall mean a country which is not a member of the EEA
- the term "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal information; and
- "Align" (or "we") means the Align Group Members.

© 2023 Align Technology, Inc. All rights reserved.

PART II: PROCESSOR OBLIGATIONS

Part II of this Policy is divided into three sections:

- Section A addresses the basic principles that Align will observe when Align collects and uses personal information as a processor.
- Section B deals with the practical commitments made by Align to the European data protection authorities when Align collects and uses personal information.
- Section C describes the third party beneficiary rights that Align has granted to individuals in its capacity as a processor under this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1A – Align will ensure that compliance with this Policy will not conflict with applicable data protection laws where they exist.

To the extent that applicable data protection law requires a higher level of protection than is provided for in this Policy, Align acknowledges that it will take precedence over this Policy.

Rule 1B – Align will co-operate and assist a controller to comply with its obligations under applicable data protection law in a reasonable time and to the extent reasonably possible.

Align will, within a reasonable time, to the extent reasonably possible and as required under its contracts with its Customers, assist Customers to comply with their obligations as controllers under applicable data protection law. This may include, for example, complying with instructions from its Customers in order to assist them to meet their obligation to keep personal information accurate and up to date, helping it to provide individuals with access to their personal information, or helping it to conduct data protection impact assessments in accordance with applicable data protection laws.

RULE 2 – ENSURING FAIRNESS AND TRANSPARENCY AND USING PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY

Rule 2A – Align will assist a controller to comply with the requirement to explain to individuals how that information will be used to the extent reasonably possible.

Align's Customers have a duty to explain to individuals, at the time their personal information is collected or shortly after, how that information will be used. This information will be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This may be done, for example, by means of a privacy statement.

Align will provide such assistance and information to its Customers as may be required under the terms of its contracts with its Customers to comply with this requirement. For example, Align may be required to provide information about any sub-processors appointed by Align to process Customer personal information on its behalf.

Rule 2B – Align will only use personal information on behalf of and in accordance with the instructions of the controller.

© 2023 Align Technology, Inc. All rights reserved.

Align will only use personal information in compliance with its Customers' instructions, as specified in its contracts with those Customers, including with regard to any international transfers of personal information.

If, for any reason, Align is unable to comply with this Rule or its obligations under this Policy in respect of any contract it may have with a Customer, Align will inform the Customer in advance of this fact. Align's Customer may then take appropriate action, such as suspend the transfer of personal information to Align and/or terminate the contract, depending upon the terms of its contract with Align.

In such circumstances, Align will act in accordance with the instructions of its Customer and return, destroy or store the personal information in a secure manner or as otherwise required in accordance with the terms of its contract with that Customer and, if requested, certify to the Customer that this has been done.

If applicable law prevents Align from returning the personal information to its Customer, Align will ensure that such information remains confidential and will not collect and use the personal information otherwise than in accordance with the instructions of its Customer.

RULE 3A – ENSURING DATA QUALITY

Rule 3A – Align will assist controllers to keep the personal information accurate and up to date.

Align will comply with any instructions from its Customers in order to assist them to comply with their obligation to keep personal information accurate and up to date.

When required to do so on instruction from its Customers, Align will delete, anonymise, update or correct personal information. Align will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

Rule 3B – Align will assist controllers to store personal information only for as long as is necessary for the purpose for which the information was initially collected.

Where a Customer instructs Align that personal information it processes on its behalf is no longer needed for the purposes for which it was collected, Align will assist our Customer to erase, restrict or anonymise that personal information without delay and in accordance with the terms of Align's contract with the Customer.

Align will also take measures to inform Group Members or third party processors to whom the personal information has been disclosed of the need to erase, restrict or anonymise that personal information.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – Align will assist controllers to comply with the rights of individuals.

Align will act in accordance with the instructions of its Customers and undertake any reasonably necessary measures to enable its Customers to comply with their duty to respect the rights of individuals. In particular, if any Group Member receives a data subject right request, the Group Member will manage such requests according to the contract with the Customer, which may include transferring the request promptly to the relevant Customer and not responding to such a request unless authorised to do so or required by law (in accordance with the Data Protection Rights Procedure in Appendix 1).

RULE 5 – ENSURING ADEQUATE PROTECTION FOR INTERNATIONAL TRANSFERS

© 2023 Align Technology, Inc. All rights reserved.

Rule 5 – Align will not transfer personal information internationally without ensuring adequate protection for the information in accordance with applicable law.

Data transfer compliance

Various data protection laws around the world, including European laws, may prohibit international transfers of personal information to third countries unless appropriate safeguards are implemented to ensure the transferred data remains protected to the standard required in the country or region from which it is originally transferred. This includes transfers of personal information to Group Members who are subject to this Processor Policy, and transfers (and onward transfers) from Group Members to third parties who are not subject to this Processor Policy.

Where these requirements exist, we will comply with them. In addition, as a processor, we will also comply with our Customers' documented instructions in respect of any international transfers of personal information (as described in Rule 2). Whenever transferring personal information internationally, or onward transferring personal information to third parties, the Privacy Office will be consulted so that they can ensure appropriate safeguards, such as standard contractual clauses (for transfers of personal information from Europe) have been implemented to protect the personal information being transferred and a Transfer Risk Assessment (as described below) has been conducted where necessary.

No Group Member may transfer personal information internationally, or onward transfer personal information, unless and until such measures as are necessary to comply with our Customers' documented instructions, and applicable data protection law rules governing international or onward transfers of personal information, have been satisfied in full.

Transfer Risk Assessments

Where EU Regulation 2016/679 (the "**GDPR**") applies to the personal information that will be transferred (or onward transferred), then before a transferring Group Member makes an international transfer (or onward transfer) of personal information to a recipient Group Member or third party data recipient (as applicable) (a **"Data Recipient"**), the Privacy Office and the transferring Group Member will coordinate with the Data Recipient to undertake a risk assessment to ensure there is no reason to believe that the laws and practices in the country where the Data Recipient will process the personal information, including any requirements to disclose personal data or measures authorising access by public authorities, will conflict with Align's obligations under this Processor Policy (a **"Transfer Risk Assessment"**).[3] The Privacy Office shall liaise with the transferring Group Member as necessary to conduct the Transfer Risk Assessment, and shall coordinate with Invisalign, S.A. to keep it informed of the Transfer Risk Assessment and its findings.

No international transfer (or onward transfer) of personal information may take place unless and until: (a) a Transfer Risk Assessment has been conducted; and (b) any additional safeguards that are identified as necessary pursuant to the Transfer Risk Assessment to protect the transfers of personal information to the Data Recipient have been implemented by the transferring Group Member and Data Recipient.

The Transfer Risk Assessment will take due account, in particular, of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal information; the economic sector in which the transfer occurs; the storage location of the data transferred;

[3] This assessment should confirm that, where the GDPR applies to the personal information that will be transferred, those laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, and are not otherwise in contradiction with this Processor Policy.

© 2023 Align Technology, Inc. All rights reserved.

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the

safeguards under this Processor Policy, including measures applied during transmission and to the processing of the personal information in the country of destination.

The Privacy Office shall inform other relevant Group Members about the findings of the Transfer Risk Assessment, so that they can apply any identified additional safeguards determined to be necessary in respect of any identical or similar transfers they make. Where the Transfer Risk Assessment concludes that it is not possible to implement additional safeguards to ensure the Data Recipient's processing in the third country will be compatible with the requirements of this Processor Policy, then the Privacy Office shall inform the transferring Group Member (and other relevant Group Members) and shall prohibit any such transfer by the Group Member(s).

The Data Recipient will use its best efforts to provide the Privacy Office and the transferring Group Member with relevant information and continue to cooperate with the Privacy Office and the transferring Group Member to ensure compliance with the requirements of this Processor Policy throughout the duration of the transfer and subsequent processing. If the Data Recipient is not a Group Member (i.e. if it is a third party Data Recipient), the Privacy Office and the transferring Group Member will exercise appropriate diligence to ensure that the Data Recipient has used such best efforts and will continue to provide such cooperation, including where appropriate by seeking contractual assurances from the Data Recipient.

The Privacy Office and the transferring Group Member will coordinate with the Data Recipient to document the Transfer Risk Assessment and make it available to the competent supervisory authority on request.

Transfer Risk Notifications

The Data Recipient will notify the Privacy Office and the transferring Group Member promptly if, at any time during which it receives or processes personal information from the transferring Group Member, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of this Processor Policy, including following a change in the laws of the third country where it receives or processes personal information or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements of this Processor Policy (a **"Transfer Risk Notification"**). If the Data Recipient is not a Group Member (i.e. if it is a third party Data Recipient), the Privacy Office and the transferring Group Member will exercise appropriate diligence to ensure that the Data Recipient will provide any such Transfer Risk Notification, including where appropriate by seeking contractual assurances from the Data Recipient. The Privacy Office shall further assess the laws and practices of any third country to which it transfers personal information on a regular basis to ensure that any such transfers do not become incompatible with the obligations under this Processor Policy. The Privacy Office or the transferring Group Member will forward the notification to the Customer.

[4] As regards the impact of such laws and practices on compliance with this Processor Policy, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers, in particular, to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the Data Recipient's processing will not be prevented from complying with the requirements of this Processor Policy, it needs to be supported by other relevant, objective elements, and it is for the Privacy Office, the transferring Group Member and Data Recipient to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Privacy Office, the transferring Group Member and Data Recipient have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

© 2023 Align Technology, Inc. All rights reserved.

Following receipt of a Transfer Risk Notification from the Data Recipient, or if the Privacy Office or the transferring Group Member otherwise have reason to believe that the Data Recipient's processing is (or is at risk of becoming) incompatible with the obligations under this Processor Policy, the Privacy Office and the transferring Group Member shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the transferring Group Member and/or Data Recipient to address the situation, if appropriate in consultation with the Customer. The Privacy Office shall instruct the transferring Group Member to suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if the transferring Group Member is instructed by the Customer or the competent supervisory authority to do so. In this case, the transferring Group Member shall be entitled to terminate its transfers of personal information to the Data Recipient, insofar as it concerns the processing of personal information under this Processor Policy (in which event, the Data Recipient will be required to return or destroy the personal information it received, as instructed by the transferring Group Member). If the transferring Group Member transfers personal information to two or more Data Recipients, the transferring Group Member may exercise this right to terminate only with respect to the relevant Data Recipient.

RULE 6 – SECURITY AND CONFIDENTIALITY

Rule 6A – Align will implement appropriate technical and organisational measures required by the applicable data protection law as specified in a contract with a controller.

European law expressly requires that where Align provides a service to a Customer which involves the collection and use of personal information, the contract between Align and its Customer imposes clear obligations dealing with the security of that information consistent with the applicable law of the European country in which the personal information was collected to ensure that Align has in place proportionate technical and organisational security measures to safeguard the personal information.

Group Members will adhere to the security and organisational measures specified in contracts with their Customers.

Rule 6B - Align will notify a controller of any security breach that affects the personal information we process on behalf of that controller.

Group Members will notify a Customer on becoming aware of any security breach that affects the personal information collected and used on behalf of that Customer in accordance with the terms of the Group Member's contract with that Customer.

Rule 6C – Align will comply with the requirements of a controller before appointing any sub-processor.

Align will seek the authorisation of its Customer to the appointment of a sub-processor in accordance with the terms of its contract with the Customer.

We will make available to our Customer up-to-date information about the sub-processors we intend to appoint in order to obtain its authorisation. If, on reviewing this information, a Customer objects to the appointment of a sub-processor, that Customer may take such steps as are consistent with the terms of its contract with us and as referred to in Rule 2B of this Processor Policy regarding the return or destruction of the personal information.

Rule 6D – Align will ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms in its contract with a controller and (ii) this Policy, and in particular that the sub-processor will adopt appropriate and equivalent security measures.

© 2023 Align Technology, Inc. All rights reserved.

Group Members will only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by Align in this Policy. In particular, such sub-processors will be able to provide appropriate technical and organisational measures that will govern their use of the personal information to which they will have access in accordance with the terms of the Group Member's contract with its Customer.

To comply with this Rule, where a sub-processor has access to personal information covered by this Policy, Align will take steps to ensure that the sub-processor has in place proportionate technical and organisational security measures to safeguard the personal information and will impose strict contractual obligations in writing on the sub-processor which provide:

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in this Policy (and in particular Rules 6A and 6B above) and with the terms of the contract Align has with its Customer in respect of the processing in question;

- that the sub-processor will act only on Align's instructions when using that information (which instructions will be consistent with the instructions of the Customer) or on the Customer's instructions; and

- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Align in this Policy and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of any international transfers of personal information.

Where one Group Member provides a service as sub-processor to another Group Member in relation to the processing of personal data in scope of this Policy, then the Group Member acting as a processor or sub-processor agrees to comply with the itemised obligations set out in these bullet points and the Data Processing Terms under Appendix 9, in addition to the obligations it is bound to comply with under this Policy.

Rule 7 – PRIVACY BY DESIGN AND DEFAULT

Rule 7 - Align will assist its Customers to apply data protection by design and by default principles.

Align will provide its products and services in a way that assist its Customers to implement data protection by design and data protection by default principles. This means that Align will implement appropriate technical and organizational measures when providing its products and services that:

- are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to protect the rights of individuals and meet the requirements of applicable data protection laws; and

- ensure that, by default, only personal information which is necessary for each specific processing purpose are collected, stored, processed and are accessible; in particular, that by default personal information is not made accessible to an indefinite number of people without the individual's intervention.

© 2023 Align Technology, Inc. All rights reserved.

SECTION B: PRACTICAL COMMITMENTS

RULE 8 – COMPLIANCE

Rule 8 – Align will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Align's Privacy Office has the responsibility to oversee and ensure day-to-day compliance with this Policy. Align has appointed an external Data Protection Officer, who enjoys management support in exercising their function and who will become involved in privacy compliance matters as relevant and will work closely with the Privacy Office. The Privacy Office's ultimate reporting line feeds into the Chief Executive Office and the Board of Directors. The Privacy Team belongs to Align's Compliance Team which in turn belongs to the broader Legal Team. Align's Privacy Office contains a network of cross-functional local center of excellence team members, throughout offices worldwide, who advise on and receive notice of local privacy issues and help to raise privacy awareness. The Privacy Office will consult matters of privacy compliance up to the Data Protection Officer, as and when this is appropriate. Align's Information Security Team, led by its Chief Information Security Officer, helps to ensure the implementation of controls necessary for privacy compliance.

In addition to its Privacy Office, Data Protection Officer and Privacy center of excellence team members, Align operates several working groups that comprise key stakeholders across various global departments. These working groups, including Align's Security Council and Align's Privacy center of excellence define the overall direction and strategy of Align's privacy practices in consultation with the Data Protection Officer, Privacy Office and Align's Board of Directors.

RULE 9 – TRAINING

Rule 9 – Align will provide appropriate and current training to staff who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools used to collect and use personal information in accordance with the Privacy Training Programme attached as Appendix 2.

RULE 10 – RECORDS

Rule 10 – Align will maintain a record of the processing activities that it conducts on behalf of a Customer in accordance with European data protection laws.

Align will maintain a record of the processing activities that it conducts on behalf of its Customer in accordance with applicable data protection laws. These records should be kept in writing (which may be in electronic form) and Align will make these records available to competent supervisory authorities upon request. The Privacy Office is responsible for ensuring that such records are maintained.

RULE 11 – AUDIT

Rule 11 – Align will comply with the Data Protection Binding Corporate Rules Policy Audit Protocol set out in Appendix 3.

RULE 12 – COMPLAINT HANDLING

Rule 12 – Align will comply with the Data Protection Binding Corporate Rules Policy Complaint Handling Procedure set out in Appendix 4.

RULE 13 – CO-OPERATION WITH DATA PROTECTION AUTHORITIES

© 2023 Align Technology, Inc. All rights reserved.

Rule 13 – Align will comply with the Data Protection Binding Corporate Rules Policy Cooperation Procedure set out in Appendix 5.

RULE 14 – UPDATES TO THE POLICY

Rule 14 – Align will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 6.

RULE 15 – CONFLICTS BETWEEN THIS POLICY AND NATIONAL LAW

Rule 15A – Where Align believes the law applicable to it prevents it from fulfilling its obligations under this Policy, it will promptly inform:

- **the controller (unless otherwise prohibited by a law enforcement authority);**
- **the Privacy Office; and**
- **the competent supervisory authority for the controller.**

When undertaking an international transfer of personal information, Group Members will comply with the requirements of Rule 5 of Part II of this Processor Policy, to minimise the likelihood and risk of any such conflict arising in the first place.

RULE 16 – GOVERNMENT REQUESTS FOR DISCLOSURE OF PERSONAL INFORMATION

Rule 16 – If a Group Member receives a legally binding request for disclosure of personal information which is subject to this Processor Policy by a public authority under the laws of a destination country outside of Europe, or of another third country, it will comply with the Government Data Request Procedure set out in Appendix 7.

If a Group Member receives a legally binding request for disclosure of personal information by a law enforcement authority or state security body which is subject to this Processor Policy, it will:

- notify the Customer promptly unless prohibited from doing so by applicable law; and
- use its best efforts to put the request on hold and notify the appropriate data protection authority competent for the Customer by complying with the requirements of its Government Data Request Procedure set out in Appendix 7.

In no event will transfers of personal information from a Group Member to any law enforcement, state security or similar public authority be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

© 2023 Align Technology, Inc. All rights reserved.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

1. Application of this Section C

This Section C applies where personal information of individuals (namely, consumers) is protected under European data protection laws (including the GDPR), for the avoidance of doubt including in relation to transfers outside of the EEA and onward transfers. This is the case when:

- those individuals' personal information is processed in the context of the activities of a third-party controller or a Group Member (acting as processor) established in Europe;
- a non-European Customer (acting as controller) or Group Member (acting as processor) offers goods and services (including free goods and services) to those individuals in Europe; or
- a non-European Customer (acting as controller) or Group Member (acting as processor) monitors the behaviour of those individuals, as far as their behaviour takes place in Europe;

and that Customer or Group Member (as applicable) then transfers those individuals' personal information to a non-European Group Member (or its sub-processor) for processing under the Processor Policy.

2. Entitlement to effective remedies

When this Section C applies, individuals have the right to pursue effective remedies in the event their personal information is processed by Align in breach of the following provisions of this Processor Policy:

- Part II Section A (Basic Principles) of this Processor Policy;
- Rules 12 (Complaint Handling), 13 (Co-operation with Data Protection Authorities), 15 (Conflicts Between this Policy and National Legislation) and 16 (Government Requests for Disclosure of Personal Information) under Part II Section B (Practical Commitments) of this Processor Policy; and
- Part II Section C (Third Party Beneficiary Rights) of this Processor Policy.

3. Individuals' third party beneficiary rights

When this Section C applies, the right for individuals to pursue remedies in relation to the matters set out in paragraph 2 apply only if either (i) the requirements at stake are specifically directed at Align as a processor in accordance with applicable data protection law (and in accordance with the guidance published by competent data protection authorities), or (ii) the individuals cannot bring a claim against a Customer because:

- the Customer has factually disappeared or ceased to exist in law or has become insolvent; and
- no successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law.

In such cases, individuals may exercise the following rights:

- *Complaints*: Individuals may make complaints to a European Group Member in accordance with Appendix 4 and/or to the European supervisory authority (i) of his or her habitual residence; (ii) of his or her place of work; or (iii) where the alleged infringement occurred;
- *Proceedings*: Individuals may bring proceedings against Invisalign, S.A. (or "**Liable BCR Member**") in accordance with Appendix 4: (i) either in the courts of Spain (being the jurisdiction of Invisalign, S.A.); (ii) the jurisdiction of the Group Member located in Europe from which the personal

© 2023 Align Technology, Inc. All rights reserved.

information was transferred; or (iii) the jurisdiction in Europe of his or her habitual residence; to enforce compliance by Align with this Policy and the appendices; and/or

- *Liability*: Individuals may seek appropriate redress from Invisalign, S.A. in accordance with Appendix 4 including the remedy of any breach of this Policy by any Group Member outside Europe (or any non-European third-party sub-processor acting on behalf of a Group Member) and, where appropriate receive compensation from Invisalign, S.A. for any material or non-material damage suffered as a result of a breach of this Policy by a Group Member in accordance with the determination of a court or other competent authority.

- *Transparency*: Individuals also have the right to obtain a copy of the Policy and the unilateral declaration entered into by Align group companies binding each company to the Policy.

Where a non-European Group Member is acting as a processor on behalf of a Customer, in the event that an individual suffers damage where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Policy, the burden of proof to show that a Group Member or any third party sub-processor which is established outside Europe and which is acting on behalf of a European Group Member is not responsible for the breach, or that no such breach took place, will rest with Invisalign, S.A.

Invisalign, S.A. will take any action necessary to remedy a breach of this Processor Policy which is caused by a non-European Group Member or a non-European sub-processor processing personal information on behalf of a Customer

Shared liability for breaches with controllers

Where Align is engaged by a Customer to conduct processing and both are responsible for harm caused by the processing in breach of this Processor Policy, Align accepts that both Align and the Customer may be held liable for the entire damage in order to ensure effective compensation of the individual.

© 2023 Align Technology, Inc. All rights reserved.

PART III: APPENDICES

APPENDIX 1

DATA SUBJECT RIGHTS PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Data Subject Rights Procedure

1. Introduction

1.1. Individuals whose personal information is processed under this Policy by Align when Align is acting on behalf of a Customer under this Processor Policy, have certain data protection rights which they may exercise by making a request to the Customer on whose behalf Align processes the personal information.

1.2. This data subject rights request procedure (the "**Procedure**") explains how Align assists any Customer to deal with a data subject rights request relating to personal information which falls into the categories in section 1.1 above (referred to as a "**request**" or "**data subject rights request**" in this Procedure).

1.3. Where a data subject rights request is subject to European data protection law because it is made with respect of personal information collected and/or used in Europe, such a request will be dealt with by Align in accordance with this Procedure, but where the applicable European data protection law differs from this Procedure, the local data protection law will prevail.

2. Individuals' Rights

2.1. An individual making a request to a controller may be entitled to the following rights, consistent with the requirements of applicable data protection laws:

(a) **The right to access**: This is a right for an individual to obtain confirmation whether a controller processes personal information about them and, if so, to be provided with details of that personal information and access to it.

(b) **The right to rectification**: This is a right for an individual to obtain rectification without undue delay of inaccurate personal information a controller may process about them.

(c) **The right to erasure**: This is a right for an individual to require a controller to erase personal information about them on certain grounds – for example, where the personal information is no longer necessary to fulfil the purposes for which it was collected.

(d) **The right to restriction**: This is a right for an individual to require a controller to restrict processing of personal information about them on certain grounds.

(e) **The right to object**: This is a right for an individual to object, on grounds relating to his or her particular situation, to a controller's processing of personal information about them, if certain grounds apply.

(f) **The right to data portability**: This is a right for an individual to receive personal information concerning them from a controller in a structured, commonly used and machine readable format and to transmit that information to another controller, if certain grounds apply.

(g) **The right to opt-out from marketing communications:** This is a right for an individual to object, in an easy-to-exercise manner and free of charge, to the use of their personal information for direct marketing purposes.

(h) **The right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects individuals' rights:** this is the right to request that a controller does not make any decision, which produces legal effects concerning an individual or that similarly significantly affects them, based solely on the automated processing of that individual's personal information, including profiling, unless such decision is: (i) necessary for entering into, or performing, a contract between a controller and that individual; (ii) authorized by applicable law (which, in the case of personal information about individuals in Europe, must be European Union or Member State law); or (iii) based on the individual's explicit consent.

2.2. When Align processes information on behalf of a Customer (for example, a customer to whom Align provides a service) Align is deemed to be a processor of the information and the Customer will be primarily responsible for meeting the legal requirements as a controller. This means that when Align acts as a processor, Align's Customers retain the responsibility to comply with applicable data protection law.

2.3. Certain data protection obligations may be passed to Align in the contracts Align has with its

© 2023 Align Technology, Inc. All rights reserved.

Customers and Align will act in accordance with the instructions of its Customers and undertake any reasonably necessary measures to enable its Customers to comply with their duty to respect the rights of individuals. Individuals often make data subject rights requests directly to an Align entity in its capacity as a processor and so in those cases, that the Align entity will transfer such request promptly to the relevant Customer, in case such Customer is known to Align. Unless instructed to do so by a Customer, Align is not obliged to refer the individual to contact the Customer directly but may explain who has responsibility to deal with a request as a matter of good practice. Align will only respond to the request (by providing the information requested or applying an exemption in accordance with applicable data protection law) if authorised by the Customer to do so.

3. Procedure

3.1. If any staff member of Align receives any data subject rights request from an individual, they will pass the communication to Align's Privacy Office who shall seek relevant business input as appropriate, (for example, Customer Service if it involves consumer data or, Align's Human Resources if it involves human resources data) upon receipt indicating the date on which it was received together with any other information which may assist the applicable department to deal with the request. The request does not have to be official or mention data protection law to qualify as a data subject rights request.

3.2. Align shall pass the request promptly to the relevant Customer, if known, in accordance with its contract terms with that Customer and will not respond to the request directly unless authorised to do so by the Customer, except, at Align's discretion, to acknowledge receipt of the correspondence and to inform the individual that the request must be addressed to the Customer, and that Align may transfer the request to the Customer if such Customer is known to Align

3.3. When Align rectifies, erases, restricts or anonymizes personal information, on instruction of a Customer when it is acting as a processor, Align will endeavor to notify the other Align entities or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

4. Questions about this Procedure

4.1. All queries relating to this Procedure are to be addressed to the Privacy Office.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 2

DESCRIPTION OF ALIGN'S PRIVACY TRAINING PROGRAMME

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

1. Privacy Training Program

1.1. Training on this Processor Policy is based upon the existing program of internal compliance within the Align group of companies.

1.2. Align trains staff members on the basic principles of data protection, confidentiality and information security and, in this connection, Align has developed mandatory electronic training courses, supplemented by live training where appropriate, to be taken by staff members. These courses are designed to be both informative and user-friendly, generating interest in the topic. Attendance of the course is monitored and enforced by Human Resources with escalation reports of non-compliance ultimately submitted to the Board of Directors.

1.3. The program provides that all staff members, including new hires and contractors, whose role will bring them into contact with personal information are required to complete the training as part of their induction program, as part of regular refresher training at least once a year, and when necessary based on changes in the law or as part of mitigation measures. Supplemental, in-person training may be provided (as necessary) to those staff members whose role requires them to access sensitive personal information.

2. Privacy training for Align staff members Align's privacy training comprises part of the mandatory employee training process that staff members will complete as a condition of their engagement. Align's Privacy Office and Information Security team have overall responsibility for the development of the training course and collaborate with Human Resources for implementation. Align's Privacy Office and Information Security team review the training from time to time to ensure that it addresses all relevant aspects of this Policy and to ensure that the training is appropriate for individuals who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information.

2.2. New staff members are educated as part of the induction process. Existing staff members will also undertake refresher training on data protection annually.

3. Summary of the training

Align's privacy-related training courses may change from time to time but are materially as follows:

A. *Course name:* **Privacy and Global Data Protection Training**

Course Description: This course provides a broad overview of Align's privacy program, policies, procedures, and expectations, including this Policy.

Target Audience: All pertinent current staff members and contractors including new hires.

Course Objectives: At the end of the course, staff members should be able to:

- Define privacy terms;
- Protect the personal information of individuals whose personal information Align maintains;
- Identify potential threats to personal information and the protections in place within Align to safeguard such data;
- Understand and comply with data protections laws, rules, and regulations in accordance with the requirements in this Policy; and
- Identify and report suspected or actual loss of personal information.
- Managing requests for access to personal information by public authorities.

B. *Course name:* **Tech Policy, Acceptable Use**

Course Description: This course educates and provides staff members/individuals with the requirements for information security at Align and the acceptable use of Align technology resources including the use of information and devices (for example, laptops, desktops, mobile phones, etc.).

Target Audience: All officers, directors, staff members, including employees, temporary workers, consultants, and contractors of Align and its subsidiaries, who, unless otherwise specified, will be referred to as "individuals".

© 2023 Align Technology, Inc. All rights reserved.

Course Objectives: At the end of this course, individuals should be able to:

- understand the importance of Information Security;
- practice responsible use of Align Technology's resources in order to protect Align, our customers, and their personal information and devices from malicious individuals;
- practice secure work environment by securing Align devices, information and workspaces;
- practice safe email and device use; use extreme caution when opening attachments, clicking links, and entering credentials;
- comply with Align's access control protocols such as securing passwords;
- understand and adhere to the protocols of working outside of an Align office;
- understand ways to report an incident and know where to go for assistance; and
- understand and implement technical measures used to keep Align safe from malware, virus, worms, ransomware etc.

C. *Course name:* **Tech Policy, Information Classification and Handling**

Course Description: This course educates staff members on the rules for classifying and handling Align's information.

Target Audience: All officers, directors, staff members, temporary workers, consultants, and contractors of Align and its subsidiaries, who, unless otherwise specified, will be referred to as "individuals".

Course Objectives: At the end of this course, individuals should be able to:

- understand the importance of protecting Align's information;
- understand Align's information classification and categories;
- understanding restricted personal information;
- comply with information security expectations internally, when acting as a vendor and when appointing third party vendors to act on Align's behalf; and
- understanding the information handling matrix and be able to distinguish non-public/confidential data from public data.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 3

DATA PROTECTION BINDING CORPORATE RULES POLICY AUDIT PROTOCOL

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Audit Protocol

1. Background

1.1. The purpose of this Processor Policy is to safeguard personal information transferred between Group Members.

1.2. The Policy requires approval from the competent supervisory authorities in the European Member States from which the personal information is transferred. One of the requirements of the competent supervisory authorities is that Align audits compliance with the Policy and satisfies certain conditions in so doing and this document describes how Align deals with such requirements.

2. Approach

2.1. Overview of audit

2.1.1. Align's Privacy Office will be responsible for ensuring independent audits are performed and, if there are indications of non-compliance, ensure verification of compliance with the Policy. Align's Privacy Office will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of Align's Data Protection Officer, and that any corrective actions are taken to ensure compliance takes place.

2.1.2. As a processor, audits of Align's compliance with the commitments made in this Processor Policy may also be carried out by or on behalf of Align's Customers in accordance with the terms of the contract Align has with its Customers in respect of such processing, and such audits may also extend to any sub-processors acting on Align's behalf in respect of such processing.

2.1.3. One of the roles of Align's Privacy Office is to provide guidance about the collection and use of personal information subject to the Policy and to assess the collection and use of personal information by Group Members for potential privacy-related risks. The collection and use of personal information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Align to ensure compliance with the Policy as required by the competent supervisory authorities, this is only one way in which Align ensures that the provisions of the Policy are observed and corrective actions taken as required.

2.2. Timing and Scope of Audit

2.2.1. Audit of the Policy will take place at least annually or on an ad hoc basis at the instigation of Align's Privacy Office, executive management, or the Board of Directors. The scope of the audit performed will be determined by Align's Privacy Office in conjunction with Align's Internal Audit Department on the basis of the risk(s) posed by the processing activities covered by the Policy to the rights of the individuals and contemporaneous factors for that year, such as processing in a given field (for example, human resources data); areas in which any complaints are received; areas of specific or new risk for the business; areas of current regulatory focus (such as data subject's rights or specific forms of processing); and/or areas of focus for Align's internal audit teams (such as procurement practices).

2.2.2. As a Processor, any audit of this Policy will take place as required under the contract in place between that Group Member and that Customer. Where a Customer on whose behalf Align processes personal information exercises its right to audit Align for compliance with this Processor Policy, the scope of the audit shall be limited to the data processing facilities and activities relating to that controller.

2.2.3. Our audit program will cover all aspects of this Policy at appropriate regular intervals and including methods and action plans ensuring that corrective actions have been implemented.

2.3. Auditors

2.3.1. Audit of the Policy will be undertaken by Align's Internal Audit Department, but reliance on work performed by other accredited internal/external auditors may be determined by Align's Privacy Office. Align's Data Protection Officer or Internal Audit Department will manage and provide quality assurance of audit work performed by others.

2.3.2. In the event that a Customer on whose behalf Align processes personal information exercises its right to audit Align for compliance with this Processor Policy, such audit may be undertaken by

© 2023 Align Technology, Inc. All rights reserved.

that controller or by independent, accredited auditors selected by that controller as stipulated in the contract between Align and that controller.

2.4. Report

2.4.1. Findings of audits of compliance with the Policy will be reported to the Privacy Office and, if necessary, to the Global Compliance and Ethics Officer and/or the General Counsel. Where appropriate, audit findings will be reported to the Board of Directors of the Liable BCR Member and, where appropriate, to Align's parent Board. In addition, Align will:

(a) disclose the results of any audit of Align's compliance with the Policy to a competent supervisory authority; and

(b) disclose the results of any audit of Align's compliance with this Processor Policy to any controller on whose behalf Align processes personal information.

In each case, Align shall make such disclosure only upon request.

2.4.2. Align's Privacy Office will be responsible for liaising with the European competent supervisory authorities for the purpose of providing the information outlined in section 2.4.1.

2.4.3. In addition, Align has agreed that where any Group Member is located within the jurisdiction of a data protection supervisory authority based in Europe, that that data protection supervisory authority may audit that Group Member for the purpose of reviewing compliance with the Policy, in accordance with the applicable law of the country in which the Group Member is located, or, in the case of a Group Member located outside Europe, in accordance with the applicable law of the European country from which the personal information is transferred under the Policy (which, when Align acts as a processor on behalf of a Customer, will be determined by the place of establishment of the controller) on giving reasonable prior notice and during business hours (unless, in accordance with applicable law, an exceptional case would prevent such reasonable prior notice and business hours to be implemented by the competent supervisory authority), with full respect to the confidentiality of the information obtained and to the trade secrets of Align, in accordance with applicable law, and in accordance with the Data Protection Binding Corporate Rules Policy Co-operation Procedure outlined under Appendix 5. Align's Privacy Office will also be responsible for liaising with the European competent supervisory authorities for this purpose.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 4

DATA PROTECTION BINDING CORPORATE RULES POLICY COMPLAINT HANDLING PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Complaint Handling Procedure

1. Introduction

1.1. The Policy safeguards personal information transferred between Group Members. The content of the Policy is determined by the competent supervisory authorities in the European Member States from which the personal information is transferred and one of their requirements is that Align will have a complaint handling procedure in place (the "**Complaint Handling Procedure**"). The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Align under the Policy is dealt with.

2. How individuals can bring complaints

2.1. Individuals can bring complaints in writing under the Policy by contacting Align Technology, Inc., attention: Privacy Office / Legal Department, 410 North Scottsdale Road, Suite 1300, Tempe, Arizona 85288. USA, Align's Customer Service Department or by emailing privacy@aligntech.com. We encourage using this point of contact, however, complaints received by other means will also be addressed. These are the contact details for all complaints made under the Policy.

3. Who handles complaints?

3.1. Where a complaint arises under the Policy in respect of the collection and use of personal information where Align is the processor in respect of that information, Align will communicate the details of the complaint to the Customer promptly and will act strictly in accordance with the terms of the contract between the Customer and Align if the Customer requires Align to deal with the complaint. Where Align will deal with the complaint, it will do so in accordance with sections 3.1.1to 3.1.4 of this Complaint Handling Procedure.

3.1.1. What is the response time?

Unless exceptional circumstances apply, Align will acknowledge receipt of a complaint to the individual concerned within five working days. It will investigate and make a substantive response within one month. If, due to the complexity of the complaint or number of requests received, a substantive response cannot be given within this period, the relevant business team (for instance, Human Resources) will, under Privacy Office's supervision, advise the complainant accordingly within the initial month period and provide a reasonable estimate for the timescale, which shall not exceed a further two months, within which a response will be provided.

3.1.2. When a complainant disputes a finding.

If the complainant disputes the response of Align or any aspect of a finding, and notifies Align accordingly, the matter will be referred to the Data Protection Officer who will review the case with the Privacy Office, if necessary, and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The Privacy Office will respond to the complainant within a reasonable time from the referral. As part of the review the Privacy Office may arrange to meet the parties in an attempt to resolve the complaint.

If the complaint is upheld, the Privacy Office will arrange for any necessary steps to be taken as a consequence. If the complaint is rejected, the Privacy Office or another department will notify the individual within the timescales set out above.

3.1.3. Complaint to a supervisory authority and/or a court of competent jurisdiction

Individuals whose personal information is collected and/or used under this Policy also have the right to complain to a European supervisory authority and/or to lodge a claim with a court of competent jurisdiction, in particular the Member State of the individual's habitual residence, place of work or place of alleged infringement and this will apply where they are not satisfied with the way in which any complaint made to Align has been dealt with. Individuals entitled to such rights will be notified accordingly as part of the Complaint Handling Procedure.

3.1.4. Proceedings before a national court

If an individual wishes to lodge a complaint against Align, on the basis that a Group Member has processed personal information in breach of the Policy or in breach of applicable data protection laws, the individual may lodge a complaint before the competent court in the European territory:

(a) in which that European Group Member is established; or

© 2023 Align Technology, Inc. All rights reserved.

(b) of where the individual has his or her habitual residence.

3.2. When a Customer ceases to exist

In circumstances where a Customer has disappeared, no longer exists or has become insolvent, and no successor entity has taken its place, individuals whose personal information is collected and/or used in accordance with European data protection law and transferred between Group Members on behalf of that Customer under the Policy have the right to complain to Align and Align will deal with such complaints in accordance with sections 3.1.1 to 3.1.3 of this Complaint Handling Procedure. In such cases, individuals also have the right to complain to a European data protection supervisory authority and/or to lodge a claim with a court of competent jurisdiction and this includes where they are not satisfied with the way in which their complaint has been resolved by Align. Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 5

DATA PROTECTION BINDING CORPORATE RULES POLICY CO-OPERATION PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Co-operation Procedure

1. Introduction

1.1. This co-operation procedure sets out the way in which Align will co-operate with the European[5] competent supervisory authorities in relation to this Processor Policy (the "**Co-operation Procedure**").

2. Co-operation Procedure

2.1. Where required, Align will make the necessary personnel available for dialogue with a European data protection supervisory authority in relation to the Policy.

2.2. Align will actively:

(a) cooperate with, and accept to be audited and to be inspected, including where necessary, on-site, by the competent supervisory authorities;

(b) abide by, any decisions made by relevant European competent supervisory authorities on any data protection law issues related to the Policy;

(c) take into account the advice of the competent European competent supervisory authorities;

(d) review and consider the views of the European Data Protection Board as outlined in its published guidance on Binding Corporate Rules for Data Processors.

2.3. Align will provide upon request (i) any information about the processing operations covered by the Policy; and (ii) copies of the results of any audit of the Policy to a relevant European data protection supervisory authority.

2.4. Align agrees to abide by a decision of the applicable data protection supervisory authority where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policy.

[5] References to Europe for the purposes of this document includes the EEA and Switzerland

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 6

DATA PROTECTION BINDING CORPORATE RULES POLICY UPDATING PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Updating Procedure

1. Introduction

1.1. This updating procedure sets out the way in which Align will communicate changes to this Processor Policy to the European competent supervisory authorities, data subjects, its Customers and to Group Members bound by the Policy (the "**Updating Procedure**").

1.2. Align will keep this Policy up-to-date and in compliance with applicable data protection laws and will update this Policy in accordance with our Updating Procedure to reflect the current situation (for instance to take into account modifications of the regulatory environment, the relevant regulatory guidance, or changes to the scope of the Policy).

2. Material changes to the Policy

2.1. Align will communicate any material changes to the Policy, that would detrimentally affect the level of protection offered by the Policy, or otherwise significantly affect the Policy (for example, by making changes to the binding nature of the Policy, change of the Liable BCR Member, etc.), promptly and in advance to the Supervisory Authorities via the Lead Supervisory Authority with a brief explanation of the reasons for the update. In this case, the competent supervisory authorities will assess whether the changes made require a new approval.

2.2. Where a change to the Policy materially affects the conditions under which Align processes personal information on behalf of any Customer under the terms of its contract with Align, Align will also communicate such information to any affected Customer. If such change is contrary to any term of the contract between Align and that Customer, Align will communicate the proposed change before it is implemented, and with sufficient notice to enable affected Customers to object.

2.3. If an affected Customer objects to the proposed change before it is implemented, Align will escalate the objection to the Privacy Office to consider, discuss with the affected Customer and resolve. If the Privacy Office cannot resolve the objection to the satisfaction of the affected Customer, then Align may choose not to implement the change or, alternatively, the affected Customer may terminate Align's data processing in accordance with the terms of its contract.

3. Other changes to the Policy

3.1. Align will communicate changes to the Policy which are administrative in nature (including changes in the list of Group Members) or other non-material changes which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure to the European competent supervisory authorities via the Lead Supervisory Authority at least once a year. Align will also provide a brief explanation to competent supervisory authorities of the reasons for any notified changes to the Policy.

3.2. Align will make available changes to the Policy which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure to any Customer on whose behalf Align processes personal information.

4. Communicating and logging changes to the Policy

4.1. Align will communicate all other changes to the Policy, whether administrative or material in nature, to all the Group Members bound by the Policy without undue delay and to the data subjects who benefit from the Policy via www.aligntech.com. The Policy contains a change log which sets out the date that the Policy is revised and the details of any revisions made.

4.2. Align's Privacy Office will maintain an up to date list of the changes made, including records of any update carried out, to the Policy, the list of Group Members bound by the Policy and a list of the sub-processors appointed by Align to process personal information on behalf of its Customers. This information will be made available online and provided to data subjects and upon request to supervisory authorities.

5. New Group Members

5.1. Align's Privacy Office will ensure that all new Group Members are bound by the Policy before a transfer of personal information to them takes place.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 7

GOVERNMENT DATA REQUEST PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Government Data Request Procedure

1. Background

1.1. Align's government data request procedure sets out Align's procedure for responding to a legally binding request for disclosure of GDPR protected personal information which is subject to this Policy by a public authority under the laws of a destination country outside of European Union, or of another third country (together the "**Requesting Authority**") to disclose personal information processed by Align (hereafter "**Data Disclosure Request**") (the "**Government Data Request Procedure**").

1.2. Where a Group Member acting as a data importer receives a Data Disclosure Request, it will handle that Data Disclosure Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal information than is required by this Government Data Request Procedure, Align will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Disclosure Requests

2.1. As a general principle, Align importers do not disclose personal information in response to a Data Disclosure Request unless either:

(a) it is under a compelling legal obligation to make such disclosure; or

(b) taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

2.2. For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, Align will notify and cooperate with the competent supervisory authorities, and where it processes the requested personal information on behalf of a Customer, the Customer, and where possible, notify the individual, in order to address the Data Disclosure Request.

3. Handling of a Data Disclosure

3.1. Receipt of a Data Disclosure Request

3.1.1. If a Group Member acting as an importer:

(i) receives a legally binding Data Disclosure Request, under the laws of the country of destination or of another third country, for disclosure of personal information and transferred pursuant to the Processor Policy, it must notify promptly the Group Member acting as the exporter and, where possible, the data subjects (if necessary with the help of the exporter). Such notification must include information about the Requesting Authority, the personal information that is requested, the legal basis on which the Data Disclosure Request is based and the response provided.

(ii) becomes aware of any direct access by public authorities to personal information transferred pursuant to the Processor Policy in accordance with the laws of the country of destination, it must notify promptly the Group Member acting as the exporter and, where possible, the data subjects (if necessary with the help of the exporter). Such notification must include all information available to the importer.

3.1.2. If prohibited from notifying the exporter or the data subjects, the importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the exporter.

3.1.3. The importer must also pass the Data Disclosure Request to Align's Legal Team immediately upon receipt, indicating the date on which it was received together with any other information which may assist Align's Legal Team to deal with the request. Align's Legal Team will, in turn, promptly inform and consult the Privacy Team about the privacy implications of the Data Disclosure Request and any data protection measures that must be taken.

3.1.4. The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Disclosure Request.

3.2. Reviewing a Data Disclosure Request

© 2023 Align Technology, Inc. All rights reserved.

3.2.1. Align's Legal Team (on behalf of the importer) will carefully review the legality of each and every Data Disclosure Request on a case-by-case basis, in particular whether the Data Disclosure Request remains within the powers granted to the Requesting Authority. Align's Legal Team will liaise with the Data Protection Officer and the Privacy Office as appropriate to determine the nature, context, validity, scope and urgency of the Data Disclosure Request, as well as its validity under applicable laws, in order to identify whether action may be needed to challenge the Data Disclosure Request.

3.3. Challenging a Data Disclosure Request

3.3.1 Align's Legal Team (on behalf of the importer), will challenge the request if, after careful assessment, it appears that there are reasonable grounds to consider that the request is unlawful under the applicable laws of the country in which the importer is located, or under applicable obligations under international law, and principles of international comity.

3.3.2 When challenging a request, Align's Legal Team, on behalf of the importer, will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal information requested until required to do so under the applicable procedural rules.

3.3.3 Where applicable, Align's Legal Team, on behalf of the importer, may appeal the decision of the Requesting Authority in accordance with the procedural laws of the country in which the importer is located.

3.4. Responding to a Data Disclosure Request

3.4.1 Align's Legal Team, on behalf of the importer, shall provide the minimum amount of personal information permissible when responding to a Data Disclosure Request, based on a reasonable interpretation of the request.

4. Notice of a Data Disclosure Request

4.1. Notice to the European Union Customer

4.1.1. Where Align is processing personal information on behalf of a European Union Customer, after assessing the nature, context, purposes, scope and urgency of the Data Disclosure Request, Align will notify and provide the Customer with the details of the Data Disclosure Request prior to disclosing any personal information, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

5. Transparency reports

5.1. The importer shall provide the exporter, at regular intervals upon request, with as much information as possible on the Data Disclosure Requests received, including the number of requests, type of data requested, requesting authorities and, outcome. If the importer is or becomes partially or completely prohibited from providing this information to the exporter, it shall, without undue delay, inform the exporter accordingly.

5.2. The importer shall preserve the abovementioned information in section 5.1 for as long as the personal information is subject to the safeguards under this Policy, and shall make it available to the competent supervisory authorities upon request.

6. Documentation

6.1. The importer shall document its legal assessment and any challenge to the Data Disclosure Request and, to the extent permissible under the national/local laws of the country where the importer is located, make the documentation available to the exporter and to the competent supervisory authorities, upon request.

7. Bulk transfer

7.1. In no event will any Group Member provide access to personal information to a Requesting Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 8

MATERIAL SCOPE OF THIS POLICY

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Material Scope of This Policy

1. Background

1.1 This Policy provides a framework for the transfer of personal information between Group Members.

1.2 This Appendix 8 sets out the material scope of the Policy. It specifies the categories of data transfers, including the nature and categories of personal information, the type of processing and its purposes, the types of individuals affected, and the third country or countries.

2. Patient data

Who transfers the personal information described in this section?	Align entities, where relevant, as detailed in the list of Group Members. Transfers made directly from a Customer directly to a Group Member as processor will also be within the scope of the Policy.
Who receives this personal information?	Align entities, where relevant, as detailed in the list of Group Members.
What categories of personal information are transferred and who are the types of individuals whose personal information is transferred?	**Patient data**: including personal information relating to patients and physicians that they choose to share with Align for processing, in particular within the context of the provision of services by Align.
What categories of sensitive personal information (if any) are transferred?	N/A
Why is this personal information transferred and how will it be used?	Align will process this personal information as instructed by its Customers, in order to provide a service to its Customers, including to: • give access physicians to Align's services at the Customer's request; • support physicians regarding their use of Align's services; and • handle any claims or queries from patients on behalf of a Customer, as relevant.
Where is this personal information processed?	Personal information is processed at all Align entity locations as listed in its Group Members or where its external processors are located.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 9

DATA PROCESSING TERMS

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Processor Policy

Data Processing Terms

1. Where a Group Member, acting as the processor, appoints another Group Member or a third party service provider (i.e. the sub-processor) to process personal information on behalf of a Customer (acting as the controller), the processing of personal information shall be governed by the following terms. In case the sub-processor is not a Group Member, these terms shall be integrated within the service level agreement that is entered into with this sub-processor.

2. Processor, respectively sub-processor shall:

2.1 Comply with applicable data protection laws when collecting, accessing and further processing personal information on behalf of the controller.

2.2 Only process the personal information in scope, on behalf of and according to the documented instructions from the controller and applicable laws for the duration and purpose of performing the services, unless required to do so by Europe or Member State law to which the processor or sub-processor is subject; in such a case, the processor or sub-processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

2.3 Immediately notify the controller if it is of the opinion that any instructions provided by the controller is in breach of any applicable data protection laws.

2.4 Hold personal information in strict confidence, and ensure that persons, including its own personnel, who are authorized to process the personal information, have committed themselves to confidentiality or are under a statutory obligation of confidentiality.

2.5 Provide sufficient guarantees to implement appropriate technical and organizational measures to meet the requirements of applicable data protection laws in accordance with Rule 6 of the Policy.

2.6 Promptly notify controller in writing, unless specifically prohibited by applicable laws, if the processor or sub-processor:

(a) receives any requests from a data subject with respect to personal information including, but not limited to requests for access and/or rectification, and all similar requests, and shall not respond to any such request unless expressly authorized to do so by controller, except to acknowledge receipt of the request;

(b) receives any complaint relating to the processing of personal information including, but not limited to, allegations that the processing infringes an individual's rights under applicable data protection laws. The processor or sub-processor shall not respond to any of such requests or complaint unless expressly authorized to do so by the controller, except to acknowledge receipt of the request;

(c) receives any request or order of a competent supervisory authority requiring it to disclose, or refrain from further processing of some or all personal information; and

(d) believes that it may no longer be able, or no longer is able, to comply with this section 2.6.

2.7 Provide all information to the controller reasonably necessary to demonstrate compliance with applicable data protection laws and reasonably assist and support the controller:

(a) in the event of an investigation by any regulator, including a data protection supervisory authority, or similar authority, if and to the extent that such investigation relates to personal information handled by the processor or sub-processor on behalf of the controller;

(a) in complying with the rights of data subjects by appropriate technical and organizational measures;

(b) in notifying and obtaining approvals from data protection authorities where required;

(c) in performing data protection impact assessments; and

(d) in consulting with data protection authorities.

2.8 Ensure that all personal information received from or on behalf of the controller is maintained in a secure manner and take all measures necessary in accordance with Rule 6 of the Policy.

2.9 In the case of a data security incident, immediately notify the controller after having become aware of the security incident. The processor or sub-processor shall, at controller's request, reasonably assist in handling the security incident.

© 2023 Align Technology, Inc. All rights reserved.

2.10 The processor shall not engage any sub-processors or third parties without the prior written consent of the controller. If any third party sub-processor shall have access to personal information, such access shall be permitted on a need–to-know basis and after the processor has entered into an agreement with such sub-processor imposing the same obligations as applicable for the processor. For this purpose, the controller specifically authorizes the processor to enter into such agreements with sub-processors for and on behalf of the controller. In case of cross-border data transfers, additional safeguards, such as EU Standard Contractual Clauses, between the processor and sub-processor shall be implemented prior to any disclosure, in accordance with Rule 5 of the Policy.

2.11 At the choice of the controller, delete or return all personal information to the controller after the end of the provision of the services relating to processing, and delete existing copies unless applicable data protection laws require the retention of the personal information.

2.12 Make available to the controller all information necessary to demonstrate compliance with the obligations under applicable data protection laws and allow for and contribute to audits, including inspections, conducted by the controller or another audit mandated by the controller.

2.13 The subject-matter and duration of the processing, the nature and purpose of the processing, the categories of data subjects and the obligations and rights of the controller shall be laid out in a separate document or legal act that is agreed between the controller and the processor.

© 2023 Align Technology, Inc. All rights reserved.