Align Technology

Data Protection Binding Corporate Rules Controller 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 4B and Appendix 2. Amendments linked to appointment of external DPO and update of the privacy training titles. Amendments with regards to certain processes, processing activities, 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.
20 December 2024	Updated to account for new BCR-C Referential - edpb_recommendations_20221_bcr-c_v2_en.pdf
18 July 2025	Updated to remove processor relevant provisions from the Appendices.
29 September 2025	Updated the scope of the policy with regards to categories of personal information transferred, the purposes of the transfers and the relevant lawful bases for processing.
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.

Contents

INTRODUCTION TO THIS POLICY

This Data Protection Binding Corporate Rules Controller Policy ("**Policy**" or "**Controller 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 for their own purposes. The list of Group Members may be found in the Investors section of the website by accessing section Documents and Charters in the Corporate Governance tab.

Scope of this Policy

This Policy applies when we process personal information as a controller and transfer personal information between Group Members (including onward transfer to other BCR members outside of the EEA). The standards described in the Controller Policy are worldwide standards that apply to all Group Members when processing personal information as a controller (or a processor on behalf of a controller Group Member) unless otherwise specified. 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.

Types of personal information within the scope of this Policy

This Policy applies to all personal information that we process as a controller including personal information processed in the course of business activities, employment administration and vendor management – such as:

- **Human resources data**: including personal information of past and current staff members [1], temporary staff and job applicants;
- **Customer relationship management data**: including personal information relating to physicians who use our services;
- **Consumer data**: including personal information relating to consumers and physicians who we market our services to and in relation to maintaining our consumer facing app;
- **Supply chain management data**: including personal information of individual contractors and of account managers and staff of third-party vendors who provide services to us; and
- **Research & Development data**: including personal information processed in connection with conducting clinical studies, training and improving models and the analysis of use of our services and products in order to develop new services and products.

More details about the material scope of this Controller Policy are provided in Appendix 8.

Our collective responsibility to comply with this Controller Policy

All Group Members and their staff will comply with and respect this Policy when collecting and using personal information for their own purposes, (or for the purposes of a controller Group Member) 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.

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 supervisory 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.

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.

Important terms used in this Policy

[1] "Staff member" includes employees and those who work on a non-permanent basis, including contingent workers, temporary and contract workers, independent contractors, consultants, professional advisors (providing support in a personal capacity), secondees, interns and other third parties engaged to carry out work for us and who have access to our premises or our internal systems.

For the purposes of this Controller 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 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.

Where will this Controller Policy be made available?

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

The Controller Policy may be found in the Investors section of the website by accessing section Documents and Charters in the Corporate Governance tab.

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

Data protection law gives people the right to control how their "**personal information**"[2] is used. When Align collects and uses the personal information of consumers, physicians, staff members, applicants and vendors this is covered and regulated by data protection law.

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/or uses information on behalf of a third party controller (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[3] that do not ensure an adequate level of data protection. Some of the countries in which Align operates are not regarded by European competent supervisory authorities as providing an adequate level of protection for individuals' data privacy rights.

WHAT IS ALIGN DOING ABOUT IT?

In order to comply with applicable European data protection law, Align will take proper steps to ensure that its use of personal information on an international basis is safe and, hence, lawful. The purpose of this Policy, therefore, 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 used and collected in Europe and transferred from Group Members within Europe to Group Members outside Europe.

Align will apply this Policy globally where Align collects, uses and transfers personal information both manually and by automatic means when the personal information relates to consumers, physicians, staff members, applicants and vendors.

This Policy applies to all Group Members and their staff worldwide and requires that Group Members who collect, use or transfer personal information as a controller (or a processor of a Group Member controller) 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 Processor Policy when they collect, use or transfer personal information as a processor of a controller which is not a Group Member. Some Group Members may be required to comply with this Policy and also the Data Protection Binding Corporate Rules Processor Policy as appropriate depending on the role they perform in relation to the personal data they handle.

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

[2] Personal information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in the GDPR.
[3] For the purposes of this Policy, reference to Europe or European means the EEA and Switzerland.

protection compliance matters, including in relation to the compliance with this Policy.

The Privacy Office is responsible for monitoring compliance with this Policy and ensuring that changes to this Policy are communicated to the Group Members and to individuals whose personal information is collected and used by Align. Align enjoys the highest level of management support for the fulfilment of this task.

If you have a complaint 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.

PART II: OBLIGATIONS UNDER THIS CONTROLLER POLICY

This Policy applies in all cases where a Group Member collects, uses and transfers personal information as a controller (or a processor on behalf of a controller Group Member).

Part II of this Policy is divided into three sections:

- Section A addresses the basic principles of European data protection law that a Group Member will observe when it collects, uses and transfers personal information as a controller.
- Section B deals with the practical commitments made by Align to the European competent supervisory authorities in connection with this Policy.
- Section C describes the third-party beneficiary rights that Align has granted to individuals under this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1 – Align will first and foremost comply with local law where it exists.

As an organisation, Align will comply with applicable law relating to personal information (e.g. in Europe, the GDPR and any local law supplementing it as amended or replaced from time to time) and will ensure that where personal information is collected and used this is done in accordance with applicable law.

Where there is no law or the law does not meet the standards set out by the Rules in this Policy, Align's position will be to collect, use and transfer personal information adhering to the Rules in this Policy.

We will ensure that we have a lawful basis for processing personal information, consistent with the requirements of applicable data protection laws. Align shall only process personal information based on the legal grounds that are detailed in Appendix 8 or 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 explain to individuals, at the time their personal information is collected, how that information will be used.

Align will ensure that individuals are told in a concise, transparent, intelligible and easily accessible form, using clear and plain language (usually by means of a privacy statement) how their personal information will be used. The information that Align has to provide includes the following ("**Fair Information Disclosures**"):

- the identity of the data controller and its contact details;
- the contact details of the data protection officer;
- the purposes of the processing for which the personal information is intended as well as the legal basis for the processing;
- where the processing is based on Align's or a third party's legitimate interests, the legitimate interests pursued by Align or by the third party;
- the recipients or categories of recipients of their personal information (if any);
- where applicable, the fact that a Group Member in Europe intends to transfer personal information to a third country or international organisation outside of Europe, and the measures that the Group

Member will take to ensure the personal information remains protected in accordance with applicable EU data protection law.

In addition to the information above, Align shall, at the time when personal information is obtained, provide individuals with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal information will be stored, or if that is not possible, the criteria used to determine that period;
- information about the individuals' rights to request access to, rectify or erase their personal information, as well as the right to restrict or object to the processing, and the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the competent supervisory authority;
- whether the provision of personal information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal information and of the possible consequences of failure to provide such information;
- the existence of automated decision-making, including profiling, and, where such decisions may have a legal effect or significantly affect the individuals whose personal information is collected, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for those individuals.

Where personal information has not been obtained directly from the individuals concerned, Align shall provide those individuals, in addition to the information above, with the following information:

- the categories of personal information that are being processed; and
- from which source the personal information originates, and if applicable, whether it came from publicly accessible sources.

This information will be provided when personal information is obtained by Align from the individual or, if not practicable, to do so at the point of collection, as soon as possible after that. In limited cases, Align may not need to provide the Fair Information Disclosures (for example, because the individual already has the information, the provision of the Fair Information Disclosures may prove impossible or involve a disproportionate effort, or where otherwise permitted by law). Where this is the case, Align shall decide what course of action is appropriate to protect the individual's rights, freedoms and legitimate interests. Where Align obtains an individual's personal information from a source other than that individual, Align will provide this information to the individual when their personal information is first recorded or, if it is to be disclosed to a third party, no later than the time when the data is first disclosed.

Align will follow this Rule 2A unless there is a legitimate basis for not doing so (for example, where it is necessary to safeguard national security or defence, for the prevention or detection of crime, taxation purposes, legal proceedings, or where otherwise permitted by law).

Rule 2B – Align will only obtain and use personal information for specified, explicit and legitimate purposes.

This rule means that Align will identify and make known the purposes for which personal information will be used (including the secondary uses and disclosures of the information) when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so as described in Rule 2A.

Rule 2C – Align may only collect and use personal information collected in Europe for a different or new purpose that is incompatible with the purposes state at Rule 2B if Align has a lawful basis for doing so.

If Align collects personal information for a specific purpose (as communicated to the individual via the relevant Fair Information Disclosure) and subsequently Align wishes to use the information for a different or new purpose which is incompatible with the original purpose, Align will ordinarily obtain the individual's consent unless it has an alternative lawful basis for the new use that is consistent with

applicable data protection law. Align must also, prior to that further processing, provide the individual with Fair Information Disclosures and any relevant information about the further processing, in accordance with this Rule 2.

RULE 3 – ENSURING DATA QUALITY

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

In order to ensure that the personal information held by Align is accurate and up to date, Align actively encourages individuals to inform Align when their personal information changes.

Align will take every reasonable step to ensure that personal information that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

Rule 3B – Align will only keep personal information for as long as is necessary for the purposes for which the personal data are processed.

Personal information will be retained and/or deleted to the extent required by applicable law, regulation and professional standards and in line with Align's Record Retention Policy as updated and amended from time to time and related procedures.

Rule 3C – Align will only keep personal information, which is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Align will identify the minimum amount of personal information that is required in order to properly fulfil its purposes.

RULE 4 – SECURITY AND CONFIDENTIALITY

Rule 4A – Align will always adhere to its IT security policies.

Align will implement appropriate technical and organizational measures to protect personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves the transmission of personal information over a network, and against all other lawful forms of processing. Such measures will take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.

Align will comply with the requirements contained in the security policies in place within Align as revised and updated from time to time together with any other security procedures relevant to a business area or function. Align will implement and comply with breach notification policies as required by applicable data protection law. In particular, Align staff members shall be under an obligation to notify without undue delay any personal information breaches to Align's Privacy Office, Align's Legal Team and/or Align's Information Security team as well as Invisalign SA. In case the Group Member is acting as a processor and becomes aware of the breach, Align staff members shall be under an obligation to notify the Group Member acting as controller.

As required by applicable data protection law, Align will notify the competent supervisory authority without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the incident unless the personal information breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where notification to the affected individuals is also required by applicable data protection law i.e. where the personal information breach is likely to result in a high risk to their rights and freedoms, they must be notified without undue delay.

Furthermore, any personal information breach should be documented (comprising the facts relating to the personal information breach, its effects and the remedial action taken) and the documentation should be made available to the competent supervisory authority on request.

Align will ensure that any staff member who has access to or is involved in the processing of personal information does so only on instructions from the relevant Group Member and under a duty of

confidentiality.

Rule 4B – Align will ensure that providers of services to Align also adopt appropriate and equivalent security measures.

Where a provider of a service to any of the Group Members has access to consumer, physician, staff member, applicant or vendor personal information (e.g. a payroll provider), strict contractual obligations, evidenced in writing must be agreed to by the service provider as set out in the Data Processing Terms in Appendix 9.

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

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5 – Align will adhere to the Data Subject Rights Procedure and will be receptive to any queries or requests made by individuals in connection with their personal information.

Individuals are entitled (by making a written request to Align) to exercise the following rights available under European Union law:

- *The right of access*: This is a right for an individual to obtain confirmation whether Align processes personal information about them and, if so, to be provided with details of that processing and access to the personal information;
- *The right to rectification*: This is a right for an individual to obtain rectification without undue delay of inaccurate personal information Align may process about them;
- *The right to erasure*: This is a right for an individual to require Align 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. If we have made the personal information public, then (taking account of available technology and the cost of implementation) we must also take reasonable steps, including technical measures, to inform third party controllers who are processing the personal information that the individual has requested the erasure by such controllers of any links to, or copy or replication of, that personal information;
- *The right to restriction*: This is a right for an individual to require Align to restrict processing of personal information about them on certain grounds;
- *The right to data portability*: This is a right for an individual to receive personal information concerning them from Align in a structured, commonly used and machine-readable format and to transmit that information to another controller, if certain grounds apply;
- *The right to object*: This is a right for an individual to object, on grounds relating to their particular situation, to processing of personal information about them, if certain grounds apply.

Where an individual wishes to exercise any of its data protection rights, Align will respect those rights in accordance with applicable data protection law and follow the steps set out in the Data Subject Rights Procedure (see Appendix 1) when dealing with them.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR OVERSEAS TRANSFERS

Rule 6 – Align will not transfer personal information internationally without ensuring appropriate safeguards for the information in accordance with the standards set out by this Policy. Align will ensure the adequate protection of any personal information that may be onward transferred outside of Europe.

Data Transfer Compliance

Various data protection laws around the world, including European laws, may prohibit international transfers of personal information to third countries without appropriate safeguards being taken 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 Controller Policy, and transfers (and onward transfers) from Group Members to third parties who

are not subject to this Controller Policy.

Where these requirements exist, we will comply with them and make individuals aware of these international transfers and onward transfers consistent with our fairness and transparency requirement in Rule 2A. When transferring personal information internationally, or onward transferring personal information to third parties, the Privacy Office will be consulted so that they can ensure that, where required in the absence of an adequacy decision, appropriate safeguards such as signing up to appropriate contractual clauses that will protect the personal information being transferred in accordance with the standards set out by this Policy and conducting a Transfer Risk Assessment (as described below) where necessary.

Suitable contractual clauses for use where personal information is to be transferred to such third parties are available from the Privacy Office and Align will make use of those contractual clauses in all such instances.

No Group Member may transfer personal information internationally, or onward transfer personal information, unless and until such measures as are necessary to comply with applicable data protection laws governing international transfers, including onward transfers, of personal information have been satisfied in full.

In the absence of an adequacy decision applicable to the recipient of personal information outside Europe, or in the absence of appropriate safeguards in place between the parties, transfers, including onward transfers, may exceptionally take place on the grounds of a legal derogation in compliance with applicable data protection law.

Transfer Risk Assessments set out in the next section will not be required if the transfer is carried out under an adequacy decision or on the grounds of a legal derogation.

Transfer Risk Assessments

Where 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 an importer 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 transfer risk assessment to assess whether the laws and practices in the country where the Data Recipient will process the personal information, including any requirements to disclose personal information or measures authorising access by public authorities, conflict with Align's obligations under this Controller Policy preventing the Data Recipient from fulfilling its obligations under this Controller Policy (a "**Transfer Risk Assessment**")[4].

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.

We will base the Transfer Impact Assessment on the understanding that the laws and practices of a third country shall respect the essence of the fundamental rights and freedoms, shall not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR (such as national security; defence; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest of the EU or of a Member State, in particular an important economic or financial interest of the EU or of a Member State, including monetary, budgetary and taxation matters, public health and social security; the protection of judicial independence and judicial proceedings; the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in certain cases referred to the GDPR; the protection of the data subject or the rights and freedoms of others; and the enforcement of civil law claims) and shall

[4] 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 Controller Policy.

not contradict this Controller Policy.

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

- the specific circumstances of the transfers or set of transfers, and the envisaged onward transfers within the same third country or to another third country including the Group Members and further recipients who are involved, the transmission channels used to transfer the personal information; the purposes of the transfer; the categories and format of the transferred personal information; the economic sector in which the transfer occurs; the location of the processing, including storage and transmission channels used;
- the laws and practices of the third country of destination – including those requiring the disclosure of personal information to public authorities and those authorising access by such authorities to personal information in transit as well as the applicable limitations and safeguards relevant in light of the specific circumstances of the transfer; [5] and
- any relevant contractual, technical or organisational safeguards that may need to be put in place to supplement the safeguards under this Controller Policy, including measures applied during transmission and to the processing of the personal information in the country of destination.

Whenever there is a need to put in place safeguards in addition to those envisaged under this Controller Policy, the exporter will inform Invisalign SA via the Privacy Office, who shall also be involved in conducting Transfer Risk Assessment.

Invisalign SA and the Privacy office shall inform all other Group Members about the findings of the Transfer Risk Assessment, requiring that they apply any identified additional safeguards determined to be necessary in respect of the same type of transfers they make or, 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 is compatible with the requirements of this Controller Policy, or if instructed by the competent supervisory authority, that the transfers at stake are suspended or ended.

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 Controller 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.

Each Group Member will document their Transfer Risk Assessments appropriately (coordinating with the Privacy Office) including what supplementary measures are selected and implemented and will make it available to the competent supervisory authority on request.

Transfer Risk Notifications

The Data Recipient must notify the Privacy Office, the exporter and Invisalign SA promptly if, at any time during which it receives or processes personal information from the exporter when using this Controller Policy as a tool for transfers, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of this Controller 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, that would prevent them from fulfilling their obligations under this Controller 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 exporter must 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, on behalf of the exporters and the importers, shall

[5] As regards the impact of such laws and practices on compliance with this Controller 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 timeframe. 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 Controller Policy, it needs to be supported by other relevant, objective elements, and it is for the Privacy Office, the transferring Group Member and the Data Recipient to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support the conclusion. In particular, the Privacy Office, the transferring Group Member and the 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.

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 Controller Policy.

Upon verification of a Transfer Risk Notification from the Data Recipient, the Group Member acting as exporter, the Privacy Office, and Invisalign SA shall promptly identify appropriate supplementary measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the exporter and/or Data Recipient to enable them to fulfil their obligations under this Controller Policy.

The exporter, along with Invisalign SA and the Privacy Office shall suspend the data transfer or set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended, if it considers that no appropriate safeguards for such transfer can be ensured to comply with the Controller Policy, or if the exporter is instructed by the competent supervisory authority to do so.

Following a suspension of a transfer in the circumstances set out above, the exporter shall terminate its transfers of personal information to the Data Recipient, insofar as it concerns the processing of personal information under this Controller Policy if the Controller Policy cannot be complied with and compliance is not restored within one month of suspension. In this event, the Data Recipient must return or destroy the personal information it received and any copies thereof, as instructed by the exporter.

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 7A – Align will only use sensitive personal information if it is necessary to use it.

Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying the individual, health data, data concerning sex life or sexual orientation and criminal convictions and offences. Sensitive personal information needs to be handled with additional care, in order to respect local customs and applicable laws. In particular, each Group Member will:

- avoid collection of sensitive personal information where it is not required for the purposes for which the data is collected or subsequently used; and
- limit access to sensitive personal information to appropriate persons (for example, by implementing measures to mask or make anonymous the information, where appropriate).

Rule 7B – Align will only use sensitive personal information where the individual's explicit consent has been obtained unless Align has an alternative legal basis for doing so consistent with the applicable data protection law of the country in which the personal information was collected.

In principle, individuals must explicitly agree to the collection and use of their sensitive personal information by Align unless Align has an alternative legal basis for doing so consistent with the applicable data protection law of the European country in which the personal information was collected. This permission to use sensitive personal information by Align will be specific, freely given, informed, unambiguous and explicit. Individuals do have the right to refuse to give consent. Where Align is reliant upon an individual's explicit consent to use sensitive personal information, Align acknowledges the right of an individual to withdraw their consent.

RULE 8 – LEGITIMISING DIRECT MARKETING

Rule 8 – Align will allow individuals to opt out of receiving marketing information.

All individuals have the data protection right to object free of charge to the use of their personal information for our direct marketing purposes and Align will honour all such opt-out requests.

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 – Align will respect individuals' rights not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them.

No evaluation of or decision about an individual which produces a legal effect or similarly significantly affects them can be based solely on the automated processing of personal information unless measures are

taken to protect the legitimate interests of individuals. Align will only take such decisions where they are:

- necessary for entering into, or performing, a contract between a Group Member and that individual;
- authorized by applicable law (which in the case of personal information about EU individuals, must be EU or Member State law); or
- based on the individual's explicit consent.

In the first and third cases above, Align will implement suitable measures to protect the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention, to express his or her view and to contest the decision.

Align will not make automated individual decisions about individuals using their sensitive personal information unless they have given explicit consent under Rule 7, or another lawful basis applies.

Rule 10 – DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN AND DEFAULT

Rule 10A - Align will carry out data protection impact assessments where processing is likely to result in a high risk to rights and freedoms of individuals and consult, where required by applicable data protection laws, with data protection authorities.

Where required by applicable data protection laws, Align will, prior to the processing, carry out data protection impact assessments ("**DPIAs**") whenever the processing of personal information, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will contain at least the following:

- A systematic description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the privacy rights of individuals; and
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal information and demonstrate compliance with applicable data protection laws.

Where the DPIA indicates that the processing would still result in a high risk to individuals in the absence of measures taken by the controller to mitigate the risks, the Group Member acting as the controller will, prior to processing, consult with the competent supervisory authority where required by applicable data protection laws.

Rule 10B - Align will apply data protection by design and by default when designing and implementing new products and systems.

When designing and implementing new products and systems which process personal information, Align will apply data protection by design and by default, where required by applicable data protection laws. This means implementing appropriate technical and organizational measures 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 is collected, stored, processed and is accessible; in particular, that by default personal information is not made accessible to an indefinite number of people without the individual's intervention.

SECTION B: PRACTICAL COMMITMENTS

Rule 11(a) – Align will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Rule 11 – COMPLIANCE

Align's Privacy Office has the responsibility to oversee and ensure day-to-day compliance with this Policy. Align has appointed 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, provided that it cannot result in a conflict of interest. The Privacy Office's ultimate reporting line feeds into the Chief Executive Office and the Board of Directors. The DPO reports to the highest management. 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 monitor training and compliance at a local level, help to raise privacy awareness, advise on and receive notice of local privacy issues, are in charge of handling local complaints from data subjects and are in charge of reporting major privacy issues to the Privacy Office. The Privacy Office will consult matters of privacy compliance up to the Data Protection Officer, as and when this is appropriate.

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, which include Align's Security Council 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 11(b) – Compliance with this Controller Policy

No transfer shall be made to a Group Member acting as an importer unless such Group Member is effectively bound by this Controller Policy and can deliver compliance.

A Group Member acting as importer shall promptly inform the exporter if it is unable to comply with this Controller Policy, for whatever reason, including the reasons described under Rule 10.

Where an importer is found to be in breach of this Controller Policy or is unable to comply with it, the Group Member acting as an exporter shall suspend the transfer to such importer.

A Group Member acting as an importer should, at the choice of the exporter, immediately return or delete all personal information in its possession that has been transferred under this Controller Policy (including any copies thereof) if:

(a) the exporter has suspended the transfer and compliance with this Controller Policy is not restored within a reasonable time, and in any event within one month of the suspension; or

(b) the importer is in substantial or persistent breach of the Controller Policy; or

(c) the importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under this Controller Policy.

The importer should certify the deletion of the personal information to the exporter.

Until all personal information is either deleted or returned, the importer shall continue to comply with the terms of this Controller Policy.

In case of local/national laws in the country of the importer that prohibit the return or deletion of the transferred personal information, the importer shall warrant that it will continue to ensure compliance with this Controller Policy and will only process the personal information to the extent and for as long as required under the local/national laws of such third country.

RULE 12 – TRAINING

Rule 12 – 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 process personal information in accordance with the Description of Align's Privacy Training Programme attached as Appendix 2.

RULE 13 – RECORDS

Rule 13 – Align will maintain a record of the processing activities that it conducts in accordance with European data protection laws.

Group Members will maintain a record of the processing activities carried out on personal information transferred under this Controller Policy 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.

These records must contain at least the following information:

(a) For controllers: the identity of the Group Member who is the controller, the purpose(s) of the processing, the categories of data subjects, the categories of personal information, the categories of recipients to whom the data is disclosed, the third country (or countries) where the personal information is transferred, the period of retention, and a general description of the technical and organisational measures applied.

(b) For processors: the identity of the controller on whose behalf the processor is acting, the categories of processing carried out on behalf of the controller, the third country (or countries) where the personal information is transferred, and a general description of the technical and organisational measures applied.

RULE 14 – AUDIT

Rule 14 – Align will comply with the Data Protection Binding Corporate Rules Policy Audit Protocol set out in Appendix 3.

RULE 15 – COMPLAINT HANDLING

Rule 15 – Align will comply with the Data Protection Binding Corporate Rules Policy Complaint Handling Procedure set out in Appendix 4.

RULE 16 – CO-OPERATION WITH COMPETENT SUPERVISORY AUTHORITIES

Rule 16 – Align will comply with the Data Protection Binding Corporate Rules Policy Co-operation Procedure set out in Appendix 5.

RULE 17 – UPDATES TO THE POLICY

Rule 17 – Align will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 6.

RULE 18 – CONFLICTS BETWEEN THIS POLICY AND NATIONAL LEGISLATION

Rule 18A – Align will ensure that where it believes that applicable law prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on its ability to comply with the Policy, Align will promptly inform the Privacy Office, the exporter and Invisalign S.A. unless otherwise prohibited by a law enforcement authority.

Rule 18B – Align will ensure that where there is a conflict between the legislation applicable to it and this Policy which is likely to have a substantial adverse effect on the guarantees provided for in this Policy, the Privacy Office will make a responsible decision in partnership with the business on the action to take and will report the problem to the competent supervisory authority with competent jurisdiction in case of doubt.

RULE 19 – GOVERNMENT ACCESS REQUESTS

Rule 18C - When undertaking an international transfer of personal information, Group Members will comply with the requirements of Rule 6, to minimise the likelihood and risk of any such conflict arising in the first place.

Rule 19 – If a Group Member, acting as an importer, receives a legally binding request for access of personal information originating in the European Union which is subject to this Controller Policy by a public authority under the laws of a destination country outside of the European Union, or of another third country, it will comply with the Government Data Request Procedure set out in Appendix 7.

RULE 20 – ACCOUNTABILITY

Rule 20 – Every Group Member acting as controller must comply, and be able to demonstrate compliance, with this Controller Policy and applicable data protection laws.

RULE 21 – TERMINATION

Rule 21 - The importer, which ceases to be bound by the Controller Policy may keep, return, or delete the personal information received under the Controller Policy.

If the data exporter and data importer agree that the data may be kept by the data importer, protection must be maintained in accordance with Chapter V of the GDPR.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

1. Application of this Section C

This Section C applies where personal information of individuals (namely, consumers, physicians, staff members, applicants and vendors) 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 Group Member, or its processor, which is established in Europe;
- a non-European Group Member offers goods and services, including free goods and services, to those individuals in Europe; or
- a non-European Group Member monitors the behaviour of those individuals, as far as their behaviour takes place in Europe.

2. Entitlement to effective remedies

When this Section C applies, individuals have the right to pursue the remedies set out in paragraph 3 of this Section C in the event their personal information is processed by Align in breach of the following provisions of this Policy:

- Parts II Section A (Basic Principles) of this Controller Policy;
- Rules 15 (Complaint Handling), 16 (Co-operation with Competent Supervisory Authorities), 18 (Conflicts Between this Policy and National Legislation) and 19 (Government Access Requests) under Part II Section B (Practical Commitments) of this Controller Policy; and
- Part II Section C (Third Party Beneficiary Rights) of this Controller Policy.

These rights to pursue effective remedies do not extend to those elements of the Controller Policy pertaining to internal mechanisms implemented within Group Members, such as but not limited to Appendix 2 (Privacy Training Program), Appendix 3(Audit Program), Appendix 6 (Procedure for Updating the Rules) and Rule 11 (Compliance) of this Controller Policy.

3. Individuals' third-party beneficiary rights

When the individual has a right to an effective remedy under paragraph 2 of this Section C, 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 competent 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. 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 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;
- *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 and, where appropriate seek 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;
- *Right to judicial remedy and redress:* Individuals have the right to an effective judicial remedy and to obtain redress and, where allowed seek compensation in case of any breach of one of the enforceable elements of these Rules. Individuals who have suffered material or non-material damage as a result of an infringement of an enforceable element of these Rules have the right to receive compensation from a Group Member for the damage suffered; data subjects may be represented by a not-for-profit body, organization or association under the conditions set out in applicable law and/or
- *Transparency*: Individuals also have the right to obtain a copy of this Policy and the Intra Group Agreement entered into by Align group companies binding each company to the Policy. Align will publish the Policy in full on its corporate website.

4. Responsibility for breaches by non- European Group Members

At any given time, Invisalign, S.A. (the "**Liable BCR Member**") accepts responsibility for and agrees to take the necessary actions to remedy the acts of other Group Members outside of Europe and pay compensation for any material or non-material damages resulting from the violation of this Policy by such Group Members.

In particular:

If an individual can establish facts which show it is likely that the damage has occurred because of a breach of this Controller Policy by a non-European Group Member, Invisalign, S.A. will have the burden of proof to show that the non-European Group Member is not responsible for the breach, or that no such breach took place.

If a Group Member outside Europe violates this Policy, the courts or other judicial authorities in Europe will have jurisdiction, and data subjects will have the rights and remedies against Invisalign, S.A. as if the violation had been caused by the latter in the Member State in which it is based, instead of the Group Member outside of Europe.

PART III: APPENDICES

APPENDIX 1

DATA SUBJECT RIGHTS PROCEDURE

Data Protection Binding Corporate Rules Controller Policy

Data Subject Rights Procedure

1. Introduction

1.1. When Align collects, uses or transfers personal information for Align's own purposes, Align is deemed to be a controller of that information and is therefore primarily responsible for meeting the requirements of applicable data protection law.

1.2. Where Align acts as a controller, individuals whose personal information is collected and/or used in Europe have certain data protection rights which they may exercise by making a request to Align.

1.3. In addition, individuals whose personal information is collected and/or used in Europe by Align acting as a controller and transferred between Align entities under this Controller Policy will also benefit from these rights and such requests will be dealt with in accordance with the terms of this data subject rights request procedure (the "**Procedure**").

1.4. This Procedure explains how Align deals with a data subject rights request relating to personal information which falls into the categories in sections 1.2 and 1.3 above (referred to as a "**request**" or "**data subject rights request**" in this Procedure).

1.5. 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. Align will assist individuals to exercise the following data protection 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. The process for handling this type of request is described further in paragraph 5 below.

(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. The process for handling this type of request is described further in paragraph 6 below.

(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. The process for handling this type of request is described further in paragraph 6 below.

(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. The process for handling this type of request is described further in paragraph 6 below.

(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. The process for handling this type of request is described further in paragraph 6 below.

(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. The process for handling this type of request is described further in paragraph 7 below.

(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 and we will honour all such opt-out requests.

(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:** We will 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 Group Member 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. In the (i) and (iii) cases above, we must implement suitable measures to protect the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention, to express his or her view and to contest the decision. We must never make automated individual decisions about individuals using their special categories of data unless they have given explicit consent or another lawful basis applies.

2.2. The request does not need to be made in writing but will be documented in our internal system.

2.3. No fee will be applied unless in accordance with local applicable law.

2.4. Align will deal with a valid request without undue delay and in any case within one (1) month of its receipt (or such shorter period as may be stipulated under local law). That period may be extended by a further two (2) months where necessary, taking into account the complexity and number of requests. Align will inform the individual of any such extension within one (1) month of receipt of the request, together with reasons for the delay.

2.5. Align is not obliged to comply with a data subject rights request unless Align is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request and to locate the information which that person seeks.

3. Procedure

3.1. Receipt of a data subject rights request where Align is a controller of the personal information requested.

3.1.1. 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.

3.1.2. The request does not have to be official or mention data protection law to qualify as a data subject rights request.

3.2. Initial steps

3.2.1. The Privacy Office shall make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

3.2.2. Align's Privacy Office (or the relevant business unit, as applicable and under the supervision of the Privacy Office) will then contact the individual in writing to confirm receipt of the data subject rights request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions applies (for example, because Align can demonstrate that the individual has made a manifestly unfounded or excessive request).

4. Exemptions to the requests made to Align as a controller

4.1. A valid request may be refused on the following grounds:

4.1.1. Where the request is made to a European Group Member and relates to the use or collection of personal information by that entity, if the refusal to provide the information is consistent with the applicable data protection laws within the jurisdiction in which that entity is located, or

4.1.2. Where the request does not fall within section 4.1.1 because it is made to a non-European Align entity and the refusal to provide the information is consistent with the exemptions to the right of subject access under current European data protection laws, or

4.1.3. if, in the opinion of Align Privacy Office a subject access request (defined herein) would: (a) prejudice the essential business interests of Align (which includes management planning, management forecasting, corporate finance or negotiations with a data subject);

(b) it is necessary to do so to safeguard, national or public security, defence, the prevention, investigation, detection and prosecution of criminal offences; or (c) for the protection of the data subject or of the rights and freedoms of others; or

4.1.4. if the personal information is held by Align in non-automated form and is not or will not become part of a filing system; or

4.1.5. where the personal information does not originate from Europe, has not been processed by any European Group Member, and the provision of the personal information requires Align to use disproportionate effort.

5. Requests for access to personal information ("subject access requests")

5.1. An individual is entitled to make a subject access request to a controller to require it to provide the following information concerning processing of their personal information:

(a) Confirmation as to whether the controller holds and is processing personal information about them;

(b) If so:

- the purposes of the processing;
- the categories of personal information concerned;
- the recipients or categories of recipient to whom the personal information has been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal information will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller, rectification or erasure of personal information or restriction of processing of personal information concerning the data subject or to object to such processing;
- the right to lodge a complaint with a competent supervisory authority;
- where the personal information is not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, and, where such decisions may have a legal effect or significantly affect the individuals whose personal information is collected, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for those individuals.

(c) Information about the individual's right to request rectification or erasure of their personal information or to restrict or object to its processing;

(d) Information about the individual's right to lodge a complaint with a competent supervisory authority;

(e) Information about the source of the personal information if it was not collected from the individual;

(f) Details about whether the personal information is subject to automated decision-making which produces legal effects concerning the individual or similarly significantly affects them; and

(g) Where personal information is transferred from Europe to a country outside of Europe, the appropriate safeguards that Align has put in place relating to such transfers in accordance with European data protection laws.

5.2. An individual is also entitled to request a copy of their personal information from the controller. Where an individual makes such a subject access request, the controller will provide that personal information to the individual in intelligible form.

5.3. The search and the response

5.4.1. Under the supervision of the Privacy Office, the relevant business unit, for example, Customer Service or Human Resources, will coordinate with Information Technology and

any other appropriate departments to conduct a search of all relevant electronic and paper filing systems.

5.4.2. The relevant business unit may refer any complex cases to the Privacy Office for advice, particularly where the request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.

5.4.3. The information requested will be collated into a readily understandable format (internal codes or identification numbers used at Align that correspond to personal information shall be translated before being disclosed). A written communication will be prepared by the appropriate business unit under the supervision of the Privacy Office, which includes the information required to be provided in response to a subject access request.

6. Requests for rectification, erasure, restriction or objection

6.1. If a request is received in relation to rectification, erasure, or objection where Align is the controller for that personal information, such a request will be considered and dealt with as appropriate by the local legal team member. In the absence of a local legal team member, such request will be considered and dealt with as appropriate by the Privacy Office.

6.2. If a request is received advising of a change in an individual's personal information where Align is the controller for that personal information, such information will be rectified or updated accordingly if Align is satisfied that there is a legal ground for doing so.

6.3. When Align rectifies, erases, restricts, or anonymizes personal information Align will notify the other Align entities to whom the personal information has been disclosed accordingly so that they can also update their records.

6.4. If the request made to Align as a controller is to restrict or cease processing that individual's personal information (for example, because the rights and freedoms of the individual are prejudiced by virtue of such processing by Align, or on the basis of other compelling legitimate grounds), the matter will be referred to the Privacy Office to assess.

7. Right to data portability

7.1. If an individual makes a data subject rights request to Align acting as controller to receive the personal information that they have provided to Align in a structured, commonly used and machine-readable format and/or to transmit directly such information to another controller (where technically feasible), Align's Privacy Office will consider and deal with the request appropriately in accordance with applicable data protection laws (and ensuring that the rights and freedoms of others are not adversely affected) insofar as the processing is based on that individual's consent or on the performance of, or steps taken at the request of the individual prior to entry into, a contract.

8. Questions about this Procedure

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

APPENDIX 2

DESCRIPTION OF ALIGN'S PRIVACY TRAINING PROGRAMME

Data Protection Binding Corporate Rules Controller Policy

1. Privacy Training Program

1.1. Training on this Controller Policy is based upon the existing program of internal compliance within the Align group of companies ("**Align**").

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

2.1. 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".

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, viruses, 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.

APPENDIX 3

DATA PROTECTION BINDING CORPORATE RULES POLICY AUDIT PROTOCOL

Data Protection Binding Corporate Rules Controller Policy

Audit Protocol

1. Background

1.1. The purpose of this Controller 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. 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. 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.

2.4. 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 disclose the results of any audit of Align's compliance with the Policy to a European competent supervisory authority. 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 authority based in Europe, that that data protection authority may audit that Group Member for the purpose of reviewing compliance with the Policy, in accordance with the applicable data protection 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 data protection law of the European country from which the personal information is transferred under the Policy 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, and in accordance with the Data Protection Binding Corporate Rules Policy Cooperation Procedure outlined under Appendix 5. Align's Privacy Office will also be responsible for liaising with the European competent supervisory authorities for this purpose.

APPENDIX 4

DATA PROTECTION BINDING CORPORATE RULES POLICY COMPLAINT HANDLING PROCEDURE

Data Protection Binding Corporate Rules Controller Policy

Complaint Handling Procedure

1. Introduction

1.1. This Controller 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. Align's Privacy Office will handle all complaints arising under the Policy in respect of the collection and use of personal information where Align is the controller of that information. Align's Privacy Office, working in conjunction with the relevant department (for example Customer Service input if it involves a consumer or, Align's Human Resources if it involves a current, previous, or potential staff member, intern, or contractor) will liaise with the applicable member/s of the business to deal with the complaint. The Privacy Office will investigate the complaint and coordinate a response.

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 data protection authority and / or a court of competent jurisdiction

Individuals whose personal information is collected and/or used and in accordance with European data protection law 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 Policies 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

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

APPENDIX 5

DATA PROTECTION BINDING CORPORATE RULES POLICY CO-OPERATION PROCEDURE

Data Protection Binding Corporate Rules Controller 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[6] competent supervisory authorities in relation to this Controller 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 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 controllers.

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 authority.

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

2.5. Any dispute related to a competent supervisory authority's exercise of supervision of compliance with the Policy will be resolved by the courts of the Member State of that supervisory authority, in accordance with that Member State's procedural law. The Group Members agree to submit themselves to the jurisdiction of these courts and, where permitted by Member State procedural law, Invisalign S.A. will appear before these courts.

[6] References to Europe for the purposes of this document includes the EEA

APPENDIX 6

DATA PROTECTION BINDING CORPORATE RULES POLICY UPDATING PROCEDURE

Data Protection Binding Corporate Rules Controller Policy

Updating Procedure

1. Introduction

1.1. This updating procedure sets out the way in which Align will communicate changes to this Controller Policy to the European competent supervisory authorities, data subjects, its clients and to the 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 Supervisory Authorities will assess whether the changes made require a new approval.

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.

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 each 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 and the list of Group Members bound by the Policy. 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.

APPENDIX 7

GOVERNMENT DATA REQUEST PROCEDURE

Data Protection Binding Corporate Rules Controller 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 Government Data Request Procedure. If applicable data protection law(s) require a higher standard of protection for personal information than is required by this 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 possible, notify the individual, in order to address the Data Disclosure Request.

3. Handling of a Data Disclosure Request

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 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 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

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. Transparency reports

4.1. 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.

4.2. The importer shall preserve the abovementioned information in paragraph 4.1 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.

5. Documentation

5.1. 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.

6. Bulk transfer

6.1. 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.

APPENDIX 8

MATERIAL SCOPE OF THIS POLICY

Data Protection Binding Corporate Rules Controller Policy

Material Scope of the Policy

1. Background

1.1 This Policy provides a framework for the transfer of personal information between Align 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, as well as the relevant lawful bases for processing.

2. Human resources data

Who transfers the personal information described in this section?	Align entities, where relevant, as detailed in the list of Group Members
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?	**Human resources data**: including personal information of past and current staff members*, temporary staff and job applicants. *"Staff member" includes employees and those who work on a non-permanent basis, including contingent workers, temporary and contract workers, independent contractors, consultants, professional advisors (providing support in a personal capacity), secondees, interns and other third parties engaged to carry out work for us and who have access to our premises or our internal systems. Categories of personal information include: • **Identifiers:** Direct and indirect identifiers including name, addresses, birth date and place, marriage status, and contact information, such as personal and work email addresses, emergency contact details for account recovery purposes, ID numbers, photo, license, passport, and information about family members including gender, birth date and certificate, and ID numbers. • **Employment or professional records:** Hiring, work background/ history, including CV, previous employers, previous job titles/positions, compensation expectations, and application form, previous professional memberships, details of qualifications, and educations, training achievements, recreation, long service, sick, personal, maternity, paternity, or other leave, behavior in the public area (such as hallways) of Align's office or other confidential areas of Align's facility, facial photos or finger prints needed to enter into specific working environments. • **Financial information:** Bank accounts, credit and debit cards, numbers, credit score, salary, bonus, commission and benefit options/entitlement, allowances, or withholdings. • **Internet or network activity:** All activities occurring on company provided devices, resources, networks, facilities, usage of data on corporate devices and applications, and other IT data like IP address, log files, and login information. Information collected from an applicant's device when the applicant visits Align's websites.

	• **Geo-location data:** Location from bade swipe entry or access, and company vehicle location. • **Commercial purchasing data:** Expense reports, or receipts related to travel, lodging, and board. • **Inferences.** Drawn from other categories, like preferences, characteristics, behavior, attitudes, background checks, professional references, or selection assessments.
What categories of sensitive personal information (if any) are transferred?	Where required by law: gender, national origin, religion, ethnicity, disabilities, health data, and social security numbers. For compliance reporting purposes, equal opportunity monitoring, payroll, and complying with anti-discrimination laws or investigations. For the administration of benefits, including health, dental, medical leave, or for compliance investigations. To fulfil legal obligations under relevant work, health, and safety laws or pursuant to public health orders issued by a government from time to time. For recruitment - on a voluntary disclosure basis, some sensitive personal information for legitimate recruitment-related purposes: for example, information about racial/ethnic origin, gender and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations (generally individual personal information is not shared in such reports); information about physical or mental conditions to consider accommodations for the recruitment process and/or subsequent job role, etc.
Why is this personal information transferred and how will it be used?	Employment administration and recruitment purposes. Align needs to process HR personal information for normal employment/engagement purposes. In summary, for management and administrative use, to enable Align to run its business and manage relationships with staff members effectively, lawfully and appropriately, including using information to comply with the employment contract or service agreement, to comply with legal requirements, pursue legitimate interests of Align, and protect Align's legal position in the event of legal proceedings. Recruitment purposes – in particular, to determine qualifications for employment and to reach a hiring decision. This includes assessing skills, qualifications, and background for a particular role, verifying information, carrying out reference checks or background checks, confirming sanction and embargo compliance, general research to verify the information that has been provided, and to generally manage the hiring process and communicate with applicants and internal stakeholders about it.
Where is this personal information processed?	Personal information is processed at all Align entity locations as listed in its Group of Members.
What are the lawful bases for processing of personal information described in this section?	Align's legal basis for processing personal information includes: • Performing a contract with you • Legitimate interests of Align • As required by law, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant • In response to lawful requests by public authorities (including for tax,

	immigration, health and safety, national security or law enforcement purposes) • Your consent, where required and to the extent allowed under applicable law • Our vital interests Align's legal basis for Processing sensitive personal information includes: • Explicit consent • Employment law • Your vital interests • Publicly available data • Legal claims

3. Customer relationship management data

Who transfers the personal information described in this section?	Align entities, where relevant, as detailed in the list of Group Members
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?	**Customer relationship management data:** including personal information relating to physicians who use our services. Personal information of Align customers ("**Customers**"), including, but not limited to, doctors, contacts at dental labs, Dental Service Organizations ("**DSO**") and DSO users, or other medical treatment institutions, such as hospitals, clinics, or other legal entities holding a "Medical Institution Practice License" or a similarly issued license by the applicable local authority, staff, students, and any other person with an Invisalign Doctor Site account, MyiTero account, or dentalXrai account. Categories of personal information include: • **Direct and Indirect Identifiers** including name, practice name and addresses, billing and shipping address, medical or dental license number and country or state, language, practice qualification information, tax ID, facial photos or images and contact information, such as personal and work email addresses, mobile phone number, and device numbers. • **Employment or Professional Records:** Employer, specialty, work background, including CV, previous professional memberships, details of dentistry practicing qualifications, and education. • **Financial Information:** Bank account number, billing, or shipping information. • **Commercial Purchasing Data:** Products purchased, received, or reviewed, history, feedback, and tendencies. • **Business Activity Data:** Invisalign and Vivera product usage, iTero scanner usage, dentalXrai usage, submission history, training history, interaction with Align technicians, and other statistics as part of Align's regular analysis and reporting to your

	DSO or group if applicable. • **Inferences:** Inferences made and attributed to or associated with a Customer regarding practice preferences, product interests, and suitability for prospective patients. • **Personal data provided by Customers, or that Customers grant us access to, in the course of Customers interactions with our business**
What categories of sensitive personal information (if any) are transferred?	N/A
Why is this personal information transferred and how will it be used?	Customer relationship management. To run Align's business efficiently and effectively, we process customer relationship data to manage accounts, enable access to products and services, and provide business and technical support, including managing customer queries and complaints. This includes delivering, developing and improving websites, applications and communications, as well as administering orders, billing and payment collection. We use this data to engage with customers and connect them with (potential) patients, share product updates and news, invite participation in surveys, feedback and online communities, and support marketing and commercial strategies. Additionally, we evaluate customer qualifications for our programs and licensing, protect our IT systems, and generate insights through feedback and analytics for product development purposes to anticipate and meet current and future customer needs and expectations, all in line and/or as required with legal obligations and the regular exercise of rights..
Where is this personal information processed?	Personal information is processed at all Align entity locations as listed in its Group of Members.
What are the lawful bases for processing of personal information described in this section?	• Legitimate interests of Align o Which can be sometimes necessary for us to do certain activities, in our own interest or the interest of a third party. Our legitimate interest can include: ▪ Gaining insight into customer use of our products or services; ▪ Developing and improving our product and service offering; ▪ Enabling us to enhance, customize or modify our communications; ▪ Informing customers about products and services we believe are relevant; ▪ If customers have made a transaction with us and have not opted-out from such communications;

	▪ Informing our marketing strategy; ▪ Improving our data security and keeping our records updated. • Contract: Where it is necessary for performing a contract, such as our Terms and Conditions, or where customers have asked us to take specific steps before entering into that contract • Compliance with a legal or regulatory obligation: For example, to comply with our legal obligations under applicable law (e.g., our transparency obligations under the US or French Sunshine Act, our complaints handling and investigation obligations under applicable medical device regulations, court orders, etc.) • Consent. • Exercise of rights in judicial or administrative procedures. • Other legal bases as permitted under local law

4. Consumer data

Who transfers the personal information described in this section?	Align entities, where relevant, as detailed in the list of Group Members
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?	**Consumer data**: including personal information relating to consumers and physicians who we market our services to and in relation to maintaining our consumer-facing app. Categories of personal information include: • **Identifiers:** e.g. name, contact details, email, postal address and pictures; data individuals provide to Align websites and apps, and to doctors. • **Geolocation:** Align websites and apps. • **Patient information, which may include treatment records or pictures or information provided to us by the data subject;** • **Internet or network activity**: Devices, Align websites and apps. **Communication data,** any data that is provided to Align in connection with requests, correspondence or enquiries.
What categories of sensitive personal information (if any) are transferred?	N/A
Why is this personal information transferred and how will it be used?	Purposes include: In relation to identifiers; • to send marketing and other communications; • to set up and manage app accounts; • to schedule appointments; • to connect individuals with an Align representative;

	• to process product orders; • identify safety issues and comply with legal requirements; • paid media targeted advertising and retargeting; and • group photos at educational events. In relation to healthcare information: • to comply with a legal obligation; • to anonymize or de-identify it for internal purposes such as research and development; • to fulfil a contract with the data subject; • to preserve evidence in litigation; • to manage correspondence with the data subjects; In relation to internet or network activity: • improve website and app design; • address IT issues; and • service advertisements. **Communication:** To review and respond to complaints or enquiries.
Where is this personal information processed?	Personal information is processed at all Align entity locations as listed in its Group of Members.
What are the lawful bases for processing of personal information described in this section?	• Legitimate interests of Align o Which can be sometimes necessary for us to do certain activities, in our own interest or the interest of a third party. Our legitimate interest can include: ▪ Gaining insights into the use of our websites, apps, products or services; ▪ Developing and improving our websites, apps, products, and service offerings; ▪ Enabling us to enhance, customize or modify our communications; ▪ Informing individuals about products and services we believe are relevant; ▪ If you have made a transaction with us and have not opted-out from such communications; ▪ Informing our marketing strategy; ▪ Improving our data security and keeping our records updated; • Contract: Where it is necessary for performing a contract (such as our Terms and Conditions), or where consumers have asked us to take specific steps before entering into that contract • Consent. • Compliance with a legal or regulatory obligation, for example to comply with our legal obligations under applicable law (for example, our transparency obligations under the US or French Sunshine Act, our complaints handling and investigation obligations

	under applicable medical device regulations, court orders, etc.) • Exercise of rights in judicial or administrative procedures. • Other legal bases as permitted under local law.

5. Supply chain management data

Who transfers the personal information described in this section?	Align entities, where relevant, as detailed in the list of Group Members
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?	**Supply chain management data**: including personal information of individual contractors and of account managers and staff of third-party vendors who provide services to us. Including: **Direct and indirect identifiers** including name, contact information, such as work email addresses and telephone number. **Financial information:** Bank account, payment and transaction details. **Communication** data.
What categories of sensitive personal information (if any) are transferred?	N/A
Why is this personal information transferred and how will it be used?	Supply chain management.
Where is this personal information processed?	Personal information is processed at all Align entity locations as listed in its Group of Members.
What are the lawful bases for processing of personal information described in this section?	• Legitimate interests to engage with and receive services from suppliers. • Performance of a contract with suppliers.

6. Research and development data

Who transfers the personal information described in this section?	Align entities, where relevant, as detailed in the list of Group Members
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?	**Research & Development data**: including personal information processed in connection with conducting clinical studies, training and improving models and the analysis of use of our services and products in order to develop new services and products. Patient data can include personal identifiers such as name, date of birth, and medical record numbers. This includes, but is not limited to, names, addresses, email addresses, identification numbers, location data, online identifiers and any relevant data as obtained with consent.
What categories of sensitive personal information (if any) are transferred?	Medical history, biometric data, lifestyle information, treatment records. Any information that is relevant to current or future health or illness including information about the provision of health services. Other personal information includes photographs, images, scans, simulations, radiographs (x-rays), impressions, and study models of teeth, mouth, and face (when they are not special category data).
Why is this personal information transferred and how will it be used?	• Research and development purposes. • Promotional purposes • Publication purposes • Clinical education purposes
Where is this personal information processed?	Personal information is processed at all Align entity locations as listed in its Group of Members.
What are the lawful bases for processing of personal information described in this section?	Consent

APPENDIX 9

DATA PROCESSING TERMS

Data Protection Binding Corporate Rules Controller Policy

Data Processing Terms

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

2. 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 is subject; in such a case, the 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 controller if it is of the opinion that any instructions provided by the controller are in breach of any applicable data protection laws.

2.4 Hold personal information in strict confidence, and ensure that persons, including their 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 4 of the Controller Policy.

2.6 Promptly notify controller in writing, unless specifically prohibited by applicable laws, if the 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 shall not respond to any such requests or complaints 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 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 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 4 of the Controller 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 shall, at controller's request, reasonably assist in handling the security incident.

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 controller and the processor, and the processor and the sub-processor respectively, shall be implemented prior to any disclosure, in accordance with Rule 6 of the Controller 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.