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.

© 2023 Align Technology, Inc. All rights reserved.

Contents

© 2023 Align Technology, Inc. All rights reserved.

INTRODUCTION TO THIS POLICY

This Data Protection Binding Corporate Rules Controller Policy ("**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.

Scope of this Policy

This Policy applies when we process personal information as a controller and transfer personal information between Group Members. The standards described in the Controller Policy are worldwide standards that apply to all Group Members when processing personal information as a controller. 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] , individual consultants, independent contractors, temporary staff and job applicants;
- **Customer relationship management data**: including personal information relating to physicians who use our services;
- **Marketing data**: including personal information relating to consumers and physicians who we market our services to and in relation to maintaining our consumer facing app; and
- **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.
- **Research & Development data**: including personal information processed in connection with conducting clinical studies, training and improving models and the analysis of consumers', customers' and physicians' use of our services and products in order to develop new services and products.

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, 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 data protection authorities and courts, and may cause harm or distress to individuals whose personal information has not been protected in accordance with the standards described in this Policy.

In recognition of the gravity of these risks, staff members who do not comply with this Policy will be subject

[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.

© 2023 Align Technology, Inc. All rights reserved.

to disciplinary action, up to and including dismissal.

Where will this Controller Policy be made available?

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

© 2023 Align Technology, Inc. All rights reserved.

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 (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 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 data protection authorities as providing an adequate level of protection for individuals' data privacy rights.

WHAT IS ALIGN DOING ABOUT IT?

In order to comply with the 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 and uses 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 will comply with the Rules set out in **Part II** of this Policy 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. Some Group Members may act as both a controller and a processor and will therefore comply with this Policy and also the Data Protection Binding Corporate Rules Processor Policy as appropriate.

FURTHER INFORMATION

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

Attention: **Privacy Office**
Email: **Privacy@aligntech.com**
Address: **Align Technology Switzerland GmbH**
Suurstoffi 22
6343 Rotkreuz
Switzerland

Align has appointed an external Data Protection Officer. Please use the contact details outlined above to contact Align's Data Protection Officer. Align's Data Protection Officer will become involved in data

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

© 2023 Align Technology, Inc. All rights reserved.

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

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

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

© 2023 Align Technology, Inc. All rights reserved.

PART II: CONTROLLER OBLIGATIONS

This Policy applies in all cases where a Group Member collects, uses and transfers personal information as a controller.

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 data protection authorities in connection with this Policy.
- Section C describes the third party beneficiary rights that Align has granted to individuals under Part II of 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 legislation relating to personal information (e.g. in Europe, the Europe's General Data Protection Regulation 2016/679 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 local 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 and use personal information adhering to the Rules in this Policy.

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 are 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 European Union law.

© 2023 Align Technology, Inc. All rights reserved.

In addition to the information above, Align shall, at the time when personal information are 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 are 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.

© 2023 Align Technology, Inc. All rights reserved.

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.

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.

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 transmission of personal information over a network, and against all other lawful forms of processing. Such measures will ensure a level of security appropriate to the risk.

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 data breaches to Align's Privacy Office, Align's Compliance Team and/or Align's Information Security team. Align will notify the supervisory authority where there is a risk to the rights and freedoms of data subjects and will notify the data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms. Furthermore, any personal data breaches should be documented (comprising the facts relating to the personal data breach, its effects and the remedial action taken) and the documentation should be made available to the supervisory authority on request.

© 2023 Align Technology, Inc. All rights reserved.

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 on the service provider that require it:

- to act only on Align's documented instructions when processing that information, including with regard to international transfers of the information;
- to ensure that any individuals who have access to the data are subject to a duty of confidentiality;
- to have in place appropriate technical and organizational security measures to safeguard the personal information;
- only to engage a sub-processor if Align has given its prior specific or general written authorization, and on condition the sub-processor agreement protects the personal information to substantially the same standard required of the service provider;
- to assist Align in ensuring compliance with its obligations as a controller under applicable data protection laws, in particular with respect to reporting data security incidents and responding to requests from individuals to exercise their data protection rights;
- to return or delete the personal information once it has completed its services; and
- to make available to Align all information it may need in order to ensure its compliance with these obligations.

Where one Group Member provides a service as processor or sub-processor to another Group Member in relation to the processing of personal data in scope of this BCR, then the Group Member acting as a processor or sub-processor agrees to comply with the itemised obligations set out in these bullet points 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;

© 2023 Align Technology, Inc. All rights reserved.

- *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 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

Data Transfer Compliance

Various data protection laws around the word, 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 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 law rules governing international or onward transfers of personal information have been satisfied in full.

Transfer Risk Assessments

Where EU Regulation 2016/679 (the **"GDPR"**) applies to the personal information that will be transferred (or onward transferred), then before a transferring Group Member makes an international transfer (or onward transfer) of personal information to a recipient Group Member or third party data recipient (as applicable) (a "**Data Recipient**"), The Privacy Office and the transferring Group Member will coordinate with the Data Recipient to undertake a risk assessment to ensure there is no reason to believe that the laws and practices in the country where the Data Recipient will process the personal information, including any requirements to disclose personal data or measures authorising access by public authorities, will conflict with Align's obligations under this Controller Policy (a "**Transfer Risk Assessment**")[4].

[4] This assessment should confirm that, where EU Regulation 2016/679 (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

© 2023 Align Technology, Inc. All rights reserved.

The Privacy Office shall liaise with the transferring Group Member as necessary to conduct the Transfer Risk Assessment, and shall coordinate with Invisalign, S.A. to keep it informed of the Transfer Risk Assessment and its findings.

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

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

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

- the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5]; and

- any relevant contractual, technical or organisational safeguards 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.

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

The Data Recipient will use its best efforts to provide the Privacy Office and the transferring Group Member with relevant information and continue to cooperate with the Privacy Office and the transferring Group Member to ensure compliance with the requirements of this 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.

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

Transfer Risk Notifications

The Data Recipient will notify the Privacy Office and the transferring Group Member promptly if, at any time during which it receives or processes personal information from the transferring Group Member, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements

contradiction with this Controller Policy.

[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 time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the Data Recipient's processing will not be prevented from complying with the requirements of this Controller Policy, it needs to be supported by other relevant, objective elements, and it is for Privacy Office, the transferring group member and Data Recipient to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, Privacy Office, the transferring group member and Data Recipient have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

© 2023 Align Technology, Inc. All rights reserved.

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) indicating an application of such laws in practice that is not in line with the requirements of 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 transferring Group Member will exercise appropriate diligence to ensure that the Data Recipient will provide any such Transfer Risk Notification, including where appropriate by seeking contractual assurances from the Data Recipient. The Privacy Office shall further assess the laws and practices of any third country to which it transfers personal information on a regular basis to ensure that any such transfers do not become incompatible with the obligations under this Controller Policy.

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

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 7A – Align will only use sensitive personal information if it is absolutely 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 local 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 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 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 explicitly. 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.

© 2023 Align Technology, Inc. All rights reserved.

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 law, 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;
- 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, Align will 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.

© 2023 Align Technology, Inc. All rights reserved.

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

SECTION B: PRACTICAL COMMITMENTS

Rule 11 – COMPLIANCE

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

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

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

RULE 12 – TRAINING

Rule 12 – Align will provide appropriate 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 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.

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

RULE 14 – AUDIT

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

© 2023 Align Technology, Inc. All rights reserved.

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 DATA PROTECTION 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 the legislation applicable to it 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 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 on the action to take and will report the problem to the data protection authority with competent jurisdiction in case of doubt.

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

RULE 19 – GOVERNMENT REQUESTS FOR DISCLOSURE OF PERSONAL INFORMATION

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

© 2023 Align Technology, Inc. All rights reserved.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

1. Application of this Section C

This Section C applies where personal information of individuals (namely, consumers, physicians, staff members, applicants and vendors) are protected under European data protection laws (including the General Data Protection Regulation). This is the case when:

- those individuals' personal information are processed in the context of the activities of a Group Member (or its third party processor) 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 (Complaints Handling), 16 (Cooperation with Data Protection Authorities), 19 (Conflicts between this Policy and national legislation) and 20 (Government requests for disclosure of personal information) under Part II Section B (Practical Commitments) of this Controller Policy; and
- Part II Section C (Third Party Beneficiary Rights) 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 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; and/or
- *Liability*: Individuals may seek appropriate redress from Invisalign, S.A. in accordance with Appendix 4 including the remedy of any breach of this Policy by any Group Member outside Europe and, where appropriate receive compensation from Invisalign, S.A. for any material or non-material damage suffered as a result of a breach of this Policy by a Group Member in accordance with the determination of a court or other competent authority.
- *Transparency*: Individuals also have the right to obtain a copy of the Policy and the unilateral declaration entered into by Align in connection with the Policy.

In the event of a claim being made in which an individual has suffered damage where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Policy, Align has agreed that the burden of proof to show that a Group Member outside Europe is not responsible for the breach, or that no such breach took place, will rest with Invisalign, S.A.

© 2023 Align Technology, Inc. All rights reserved.

PART III: APPENDICES

APPENDIX 1

DATA SUBJECT RIGHTS PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy/Data Protection Binding Corporate Rules Processor 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 data protection law.

1.2. Where Align acts as a controller, individuals whose personal information is collected and/or used in Europe[6] 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 the Align Data Protection Binding Corporate Rules 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 ("**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 "**valid request**" in this Procedure).

1.5. Where a data subject rights request is subject to European data protection law because it is made in 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 ground 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.

[6] In this policy Europe means the EEA plus Switzerland.

© 2023 Align Technology, Inc. All rights reserved.

(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.

2.2. The request does not need to be made in writing.

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 right 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 right 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 data protection law 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

© 2023 Align Technology, Inc. All rights reserved.

to the right of subject access under current EU data protection laws, or

4.1.3. if, in the opinion of Align compliance with a subject access request 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 data ("subject access requests")

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

(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 data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data 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 data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are 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 are 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 data protection authority;

© 2023 Align Technology, Inc. All rights reserved.

(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 request, the controller will provide that personal information to the individual in intelligible form.

5.3. Subject access requests made to Align where Align is a processor of the personal information requested

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

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

5.4. 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 covering letter 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

© 2023 Align Technology, Inc. All rights reserved.

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 anonymises personal information, either in its capacity as controller or on instruction of a client when it is acting as a processor, Align will notify the other Align entities or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

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 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.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 2

DESCRIPTION OF ALIGN'S PRIVACY TRAINING PROGRAMME

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy/Data Protection Binding Corporate Rules Processor Policy

Privacy Training Programme

Training on Align's Data Protection Binding Corporate Rules Controller Policy and Data Protection Binding Corporate Rules Processor Policy (together the "**BCR**") is based upon the existing programme of internal compliance within the Invisalign, S.A. group of companies ("**Align**").

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.

The programme provides that all staff members , including new hires and contractors, whose role will bring them into contact with personal data are required to complete the training as part of their induction programme, as part of regular refresher training, 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 data.

Privacy training for Align staff members

Align's privacy training comprises part of the mandatory employee training process that staff members will complete as a condition of their engagement. Align's Privacy Office and Information Security team have overall responsibility for the development of the training course and collaborate with Human Resources for implementation. Align's Privacy Office and Information Security team review the training from time to time to ensure that it addresses all relevant aspects of the BCR 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.

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

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 the BCR.

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 the BCR; and

© 2023 Align Technology, Inc. All rights reserved.

- Identify and report suspected or actual loss of personal information.

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 & 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
- Understand and implement technical measures used to keep Align safe from malware, virus, worms ransomware etc

C. *Course name:* **Tech Policy, Information Classification & 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.

© 2023 Align Technology, Inc. All rights reserved.

- Understanding the information handling matrix and be able to distinguish non-public/confidential data from public data.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 3

DATA PROTECTION BINDING CORPORATE RULES POLICY AUDIT PROTOCOL

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy/Data Protection Binding Corporate Rules Processor Policy

Audit Protocol

1. Background

1.1. The purpose of the Data Protection Binding Corporate Rules Processor Policy and Data Protection Binding Corporate Rules Controller Policy (together the "Policies") is to safeguard personal information transferred between Align group members ("Group Members").

1.2. The Policies require approval from the data protection authorities in the European Member States from which the personal information is transferred. One of the requirements of the data protection authorities is that Align audits compliance with the Policies 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 that fully address the Policies. 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 take place.

2.1.2. To the extent that Align acts as a processor, audits of Align's compliance with the commitments made in the Data Protection Binding Corporate Rules Processor Policy may also be carried out by or on behalf of Align's clients in accordance with the terms of the contract Align has with its clients in respect of such processing, and such audits may also extend to any sub-processors acting on Align's behalf in respect of such processing.

2.1.3. One of the roles of Align's Privacy Office is to provide guidance about the collection and use of personal information subject to the Policies 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 Policies as required by the data protection authorities, this is only one way in which Align ensures that the provisions of the Policies are observed and corrective actions taken as required.

2.2. Timing and Scope of Audit

2.2.1. Audit of the Policies will take place at least annually or at the instigation of Align's Privacy Office, executive management, or the Board of Directors. The scope of the audit performed will be decided by Align's Privacy Office in conjunction with Align's Internal Audit Department in light of 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. To the extent that a Group Member processes personal information on behalf of a third party controller, audit of the Data Protection Binding Corporate Rules Processor Policy will take place as required under the contract in place between that Group Member and that third party controller. Where a third party controller on whose behalf Align processes personal information exercises its right to audit Align for compliance with the Data Protection Binding Corporate Rules Processor Policy, the scope of the audit shall be limited to the data processing facilities and activities relating to that controller.

2.3. Auditors

© 2023 Align Technology, Inc. All rights reserved.

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

2.3.2. In the event that a third party controller on whose behalf Align processes personal information exercises its right to audit Align for compliance with the Data Protection Binding Corporate Rules Processor Policy, such audit may be undertaken by that controller or by independent, accredited auditors selected by that controller as stipulated in the contract between Align and that controller.

2.4. Report

2.4.1. Findings of audits of compliance with the Policies will be reported to the Privacy Office and, if necessary, to the Global Compliance and Ethics Officer and/or the General Counsel. Any material audit findings will be reported to the Board of Directors. In addition, Align will:

(a) disclose the results of any audit of Align's compliance with the Policies to a competent European data protection authority; and

(b) disclose the results of any audit of Align's compliance with the Data Protection Binding Corporate Rules Processor Policy to any controller on whose behalf Align processes personal information;

In each case, Align shall make such disclosure only upon request, in accordance with applicable law, and with respect for the confidentiality and trade secrets of the information provided.

2.4.2. Align's Privacy Office will be responsible for liaising with the European data protection 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 Policies, in accordance with the applicable law of the country in which the Group Member is located, or, in the case of a Group Member located outside Europe, in accordance with the applicable law of the European country from which the personal information is transferred under the Policies (which, when Align acts as a processor on behalf of a third party controller, will be determined by the place of establishment of the controller) on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Align, and in accordance with the Binding Corporate Rules: Cooperation Procedure. Align's Privacy Office will also be responsible for liaising with the European data protection authorities for this purpose.

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 4

DATA PROTECTION BINDING CORPORATE RULES POLICY COMPLAINT HANDLING PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy/Data Protection Binding Corporate Rules Processor Policy

Complaint Handling Procedure

1. Introduction

1.1. The Data Protection Binding Corporate Rules Controller Policy ("**Controller Policy**") and the Data Protection Binding Corporate Rules Processor Policy ("**Processor Policy**") (together the "**Policies**") safeguard personal information transferred between the Align group members ("**Group Members**"). The content of the Policies is determined by the data protection 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 purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Align under the Policies are dealt with.

2. How individuals can bring complaints

2.1. Individuals can bring complaints in writing under the Policies by contacting Align's Customer Service Department or by emailing privacy@aligntech.com. These are the contact details for all complaints made under the Policies whether Align is collecting and/or using personal information on its own behalf or on behalf of a client.

3. Who handles complaints?

3.1. Complaints where Align is a controller

3.1.1. Align's Privacy Office will handle all complaints arising under the Controller 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 Privacy center of excellence, who represent relevant various business and support units, to deal with the complaint. Members of the Privacy Working Group will function as the Departmental Contacts to investigate the complaint and coordinate a response.

3.1.2. What is the response time?

Unless exceptional circumstances apply, Align will acknowledge receipt of a complaint to the individual concerned within 5 working days. It will investigate and make a substantive response within one month. If, due to the complexity of the complaint and number of requests, 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 and provide a reasonable estimate for the timescale within which a response will be provided.

3.1.3. When a complainant disputes a finding

If the complainant disputes the response of the Departmental Contact or Customer Service (or the individual or department within Align tasked by the Legal Team with resolving the complaint) 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.

© 2023 Align Technology, Inc. All rights reserved.

3.1.4. Complaint to a data protection authority

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 data protection authority and/or to lodge a claim with a court of competent jurisdiction 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.

3.1.5. Proceedings before a national court

If an individual wishes to commence court proceedings against Align, on the basis that a European Group Member has processed personal information in breach of the Policies or in breach of applicable data protection laws, then he or she may commence proceedings against that European Group Member in the European territory:

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

(b) of his or her habitual residence.

3.2. Complaints where Align is a processor

3.2.1. Where a complaint arises under the Processor Policy in respect of the collection and use of personal information where Align is the processor in respect of that information, Align will communicate the details of the complaint to the client promptly and will act strictly in accordance with the terms of the contract between the client and Align if the client requires Align to deal with the complaint.

3.2.2. When a client ceases to exist

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

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 5

DATA PROTECTION BINDING CORPORATE RULES POLICY CO-OPERATION PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy/Data Protection Binding Corporate Rules Processor Policy

Co-operation Procedure

1. Introduction

1.1. This Co-operation Procedure sets out the way in which Align will co-operate with the European[7] data protection authorities in relation to the Data Protection Binding Corporate Rules Controller Policy and the Data Protection Binding Corporate Rules Processor Policy (together the "**Policies**").

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 Policies.

2.2. Align will actively review and consider:

(a) any decisions made by relevant European data protection authorities on any data protection law issues that may affect the Policies; and

(b) the views of the European Data Protection Board as outlined in its published guidance on Binding Corporate Rules for data controllers and Binding Corporate Rules for data processors.

2.3. Subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Align will provide upon request copies of the results of any audit of the Policies to a relevant European data protection authority.

2.4. Where any Align group member ("**Group Member**") is located within the jurisdiction of a data protection authority based in Europe, Align agrees that that particular data protection authority may audit that Group Member for the purpose of reviewing compliance with the Policies, in accordance with the applicable law of the country in which the Group Member is located, or, in the case of a Group Member located outside Europe, in accordance with the applicable law of the European country from which the personal information is transferred under the Policies (which, when Align acts as a processor on behalf of a third party controller, will be determined by the place of establishment of the controller) on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Align.

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

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

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 6

DATA PROTECTION BINDING CORPORATE RULES POLICY UPDATING PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy/Data Protection Binding Corporate Rules Processor Policy

Updating Procedure

1. Introduction

1.1. This Data Protection Binding Corporate Rules Updating Procedure sets out the way in which Align will communicate changes to the Data Protection Binding Corporate Rules Controller Policy ("**Controller Policy**") and to the Data Protection Binding Corporate Rules Processor Policy ("**Processor Policy**") (together the "**Policies**") to the European[8] data protection authorities, data subjects, its clients and to the Align group members ("**Group Members**") bound by the Policies.

2. Material changes to the Policies

2.1. Align will communicate any material changes to the Policies as soon as is reasonably practical to the relevant supervisory authority, via the competent supervisory authority.

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

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

3. Administrative changes to the Policies

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

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

4. Communicating and logging changes to the Policies

4.1. Align will communicate all changes to the Policies, whether administrative or material in nature, to the Group Members bound by the Policies without undue delay and to the data subjects who benefit from the Policies via www.aligntech.com. The Policies contain 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 to the Policies, the list of Group Members bound by the Policies and a list of the sub-processors appointed by Align to process personal information on behalf of its clients. This information will be available on request from Align.

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

© 2023 Align Technology, Inc. All rights reserved.

5. New Group Members

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

© 2023 Align Technology, Inc. All rights reserved.

APPENDIX 7

GOVERNMENT DATA REQUEST PROCEDURE

© 2023 Align Technology, Inc. All rights reserved.

Data Protection Binding Corporate Rules Controller Policy

Government Data Request Procedure

1. Background

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

1.2. Where Align receives a Data Disclosure Request, it will handle that Data Disclosure Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal information than is required by this 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 does 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 data protection authorities (and where it processes the requested personal information on behalf of a client, the client) in order to address the Data Disclosure Request.

3. Handling of a Data Disclosure

3.1. Receipt of a Data Disclosure Request

3.1.1. If an Align Group Member receives a Data Disclosure Request, the recipient of the request will pass it 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.

3.1.2. 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. Initial steps

3.2.1. Align's Legal Team will carefully review each and every Data Disclosure Request on a case-by-case basis. Align's Legal Team will liaise with the Data Protection Officer as appropriate to deal with the request to determine the nature, context, purposes, 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.

4. Notice of a Data Disclosure Request

4.1. Notice to the client

4.1.1. Where Align is processing personal information on behalf of a client, after assessing the nature, context, purposes, scope and urgency of the Data Protection Request, Align will notify and provide

© 2023 Align Technology, Inc. All rights reserved.

the client with the details of the Data Disclosure Request prior to disclosing any personal information, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

4.2. Notice to the competent Data Protection Authorities

4.2.1. Align will also put the request on hold in order to notify and consult with the competent Data Protection Authorities, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

4.2.2. Where Align is prohibited from notifying the competent Data Protection Authorities and suspending the request, Align will use its best efforts (taking into account the nature, context, purposes, scope and urgency of the request) to inform the Requesting Authority about its obligations under applicable data protection law and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that Align can consult with the competent Data Protection Authorities, which may also, in appropriate circumstances, include seeking a court order to this effect. Align will maintain a written record of the efforts it takes.

5. Transparency reports

5.1. If, despite having used its best efforts, Align is not in a position to notify the competent Data Protection Authorities, Align commits to preparing an annual report (a "**Transparency Report"),** which reflects to the extent permitted by applicable laws, the number and type of Data Disclosure Requests it has received for the preceding year and the Requesting Authorities who made those requests. Align shall provide this report to the lead data protection authority which authorized its BCR (and any other data protection authorities that the lead authority may direct) once a year.

6. Bulk transfer

6.1. In no event will any group member transfer personal information to a Requesting Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

© 2023 Align Technology, Inc. All rights reserved.