

Align Technology

Data Protection Binding Corporate Rules
Processor Policy

Confidential

Contents

INTRODUCTION TO THIS POLICY	3
PART I: BACKGROUND AND ACTIONS	4
PART II: PROCESSOR OBLIGATIONS	6
PART III: APPENDICES	12

INTRODUCTION TO THIS POLICY

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

This Policy applies to all personal information collected and used as part of the regular business activities of Align in the course of providing services to a controller, regardless of whether the controller is a third party or another Group Member (equally referred to as the "**client**" in this Policy), and Group Members must comply with and respect this Policy when collecting and using personal information in their capacity as service providers.

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

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

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

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

When, on the other hand, an organisation collects and uses information on behalf of a third party or a different member of its corporate group (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 Europe² that do not ensure an adequate level of data protection. Some of the countries in which Align operates are not regarded by European data protection authorities as providing an adequate level of protection of individuals’ data privacy rights.

When Align acts as a processor, Align's clients retain the responsibility to comply with European data protection law. When a Group Member acts as a processor in circumstances where the controller is another Group Member located in Europe, the Group Member acting as controller will retain the responsibility to comply with European data protection law.

In practical terms, this means that those acting as controllers in Europe (whether a Group Member or an external client) must pass certain data protection obligations on to any processor which collects and uses personal information outside of Europe on their behalf in order to overcome the legal restrictions on international data transfers.

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

WHAT IS ALIGN DOING ABOUT IT?

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

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

¹ Personal information means any information relating to an identified or identifiable natural person in line with the definition of “personal data” in EU Directive 95/46/EC.

² For the purpose of this Policy reference to Europe means the European Economic Area and Switzerland.

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

Align will apply this Policy globally where Align collects and uses personal information as a processor both manually and by automatic means when such personal information originates from Europe as identified in the contract with the client. For example, this Policy applies whenever Align collects and uses patients' personal information as a processor on behalf of its European physician clients who are the controllers of those patients' personal information. It also applies whenever one Group Member collects and uses employee, consumer or vendor personal information in the context of providing services to another Group Member.

This Policy applies to all Group Members and their staff worldwide and requires that Group Members who collect, use or transfer personal information to provide services to a third party as a processor or who provide a service to other Group Members in their capacity as a processor must 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 must comply with the Data Protection Binding Corporate Rules Controller Policy when they collect, use and transfer personal information as a controller. Some Group Members may act as both a controller and a processor and must therefore comply with this Policy and also the Data Protection Binding Corporate Rules Controller Policy as appropriate.

FURTHER INFORMATION

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

Attention:	Privacy Counsel
Email:	Privacy@aligntech.com
Address:	2560 Orchard Parkway San Jose, CA 95131

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

If you are unhappy about the way in which Align has used your personal information, Align has a separate complaint handling procedure which is set out in Part III, Appendix 3.

PART II: PROCESSOR OBLIGATIONS

Part II of this Policy is divided into three sections:

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

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

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

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

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

Align will, within a reasonable time, to the extent reasonably possible and as required under its contracts with its clients, assist clients to comply with their obligations as controllers under applicable data protection law. This may include, for example, complying with instructions from its clients in order to assist them to meet their obligation to keep personal information accurate and up to date.

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

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

Align's clients have a duty to explain to individuals, at the time their personal information is collected or shortly after, how that information will be used. This may be done, for example, by means of a privacy statement.

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

Rule 2B - Align will only use personal information in accordance with the instructions of the controller.

Align will only use personal information in compliance with its clients' instructions, as specified in its contracts with those clients.

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

In such circumstances, Align will act in accordance with the instructions of its client and return, destroy or store the personal information in a secure manner or as otherwise required in accordance with the terms of its contract with that client.

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

RULE 3 - DATA QUALITY AND PROPORTIONALITY

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

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

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

RULE 4 - RESPECTING INDIVIDUALS' RIGHTS

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

Align will act in accordance with the instructions of its clients and undertake any reasonably necessary measures to enable its clients to comply with their duty to respect the rights of individuals. In particular, if any Group Member receives a subject access request, the Group Member will manage such requests according to the contract with the client, which may include transferring the request promptly to the relevant client and not responding to such a request unless authorised to do so or required by law.

RULE 5 - SECURITY AND CONFIDENTIALITY

Rule 5A - Align will adhere to the security and organisational measures required by the applicable data protection law as specified in a contract with a controller.

European law expressly requires that where Align provides a service to a client which involves the collection and use of personal information, the contract between Align and its client imposes clear obligations dealing

with the security of that information consistent with the applicable law of the European country in which the personal information was collected to ensure that Align has in place proportionate technical and organisational security measures to safeguard the personal information.

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

Rule 5B - Align will notify a controller of any security breach in accordance with the terms of the contract with that controller.

Group Members will notify a client of any security breach in relation to personal information collected and used on behalf of that client in accordance with the terms of the Group Member's contract with that client.

Rule 5C - Align will comply with the requirements of a controller before appointing any sub-processor.

Align will inform its clients before appointing a sub-processor to carry out processing on behalf of a client of Align and seek the consent of its client to the appointment of a sub-processor in accordance with the terms of its contract with the client.

Rule 5D - Align will ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms in its contract with a controller and (ii) this Policy, and in particular that the sub-processor will adopt appropriate and equivalent security measures.

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

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

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in this Policy (and in particular Rules 5A and 5B above) and with the terms of the contract Align has with its client in respect of the processing in question;
- that the sub-processor will act only on Align's instructions when using that information; and
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Align in this Policy.

SECTION B: PRACTICAL COMMITMENTS

RULE 6 - COMPLIANCE

Rule 6 - Align will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Align has appointed a Privacy Counsel to oversee and ensure day-to-day compliance with this Policy, whose ultimate reporting line feeds into the Chief Executive Office and the Board of Directors. The Privacy Counsel is supported by Align's network of cross-functional local Privacy Champions throughout all offices worldwide, who advise on and receive notice of local privacy issues and help to raise privacy awareness. Local Privacy Champions will escalate matters of privacy compliance up to the Privacy Counsel, as and when this is appropriate.

In addition to its Privacy Counsel and Privacy Champions, Align operates a Privacy Working Group that comprises key stakeholders across various global departments, including Marketing, IT, Research and Development, Sales, Operations, Finance, HR, Legal and Regulatory. The Privacy Working group defines the overall direction and strategy of Align's privacy practices in consultation with the Privacy Counsel and Align's Board of Directors.

RULE 7 - TRAINING

Rule 7 - 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 collect and use personal information in accordance with the Privacy Training Programme attached as Appendix 1.

RULE 8 - AUDIT

Rule 8 - Align will comply with the Data Protection Binding Corporate Rules Policy Audit Protocol set out in Appendix 2.

RULE 9 - COMPLAINTS

Rule 9 - Align will comply with the Data Protection Binding Corporate Rules Policy Complaint Handling Policy set out in Appendix 3.

RULE 10 - CO-OPERATION WITH DPAs

Rule 10 - Align will comply with the Data Protection Binding Corporate Rules Policy Co-operation Procedure set out in Appendix 4.

RULE 11 – UPDATES TO THE POLICY

Rule 11 – Align will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 5.

RULE 12 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 12A – Where Align believes the legislation applicable to it prevents it from fulfilling its obligations under this Policy, it will promptly inform:

- the controller (unless otherwise prohibited by a law enforcement authority);
- Align's Privacy Counsel; and
- the data protection authority competent for the controller.

Rule 12B – Where Align receives a legally binding request for disclosure of personal information which is subject to this Policy, Align will notify the controller unless prohibited from doing so by a law enforcement authority. Align will also consider whether to put the request on hold and notify the appropriate data protection authority competent for the controller and, in addition, the Dutch data protection authority in its capacity as lead authority for this Data Protection Binding Corporate Rules for Processors Policy.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Where personal information is transferred under this Policy and where: (i) the individual whose personal information is transferred is unable to bring a claim against the controller for breach of the Policy by a Group Member acting as a processor because the controller has factually disappeared or ceased to exist in law or has become insolvent; and (ii) no successor entity has assumed the entire legal obligations of the controller by contract or by operation of law, that individual will have the following third party beneficiary rights;

- (a) *Enforcement of compliance*: to seek enforcement of compliance with this Policy;
- (b) *Complaints*: to make a complaint to a European data protection authority of competent jurisdiction and/or to a Group Member in Europe;
- (c) *Liability*: to bring proceedings against Align Technology B.V. in:
 - (i) the courts of the Netherlands;
 - (ii) in the jurisdiction of the European Group Member from which the personal information was transferred; or
 - (iii) in the jurisdiction of the European Member State where the individual resides;
- (d) *Compensation*: where appropriate, to receive compensation from Align Technology B.V. for any damage suffered as a result of a breach of this Policy by:

- (i) any non- European Group Member; or
- (ii) any non-European sub-processor acting on behalf of Align

in accordance with the determination of the court or other competent authority;

- (e) *Transparency*: to obtain a copy of this Policy and the unilateral declaration.

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

Align Technology B.V. will take any action necessary to remedy a breach of the Data Protection Binding Corporate Rules for Processors Policy which is caused by a non-European Group Member or a non-European sub-processor processing personal information on behalf of a client.

PART III: APPENDICES

APPENDIX 1

DESCRIPTION OF ALIGN'S PRIVACY TRAINING PROGRAMME

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 Align Technology, Inc. group of companies ("**Align**").

Align trains employees 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 employees. 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 employees, 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 training may be provided (as necessary) to those employees whose role requires them to access sensitive personal data.

Privacy training for Align employees

Align's privacy training comprises part of the mandatory employee training process that employees must complete as a condition of their employment. Align's Privacy Counsel and Information Security team have overall responsibility for the development of the training course and collaborate with Human Resources for implementation. Align's Privacy Counsel 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 employees are educated as part of the induction process. Existing employees must also undertake refresher training on data protection annually.

Summary of the training

Align's privacy-related training courses are:

A. **Course name: Privacy at Align**

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 employees and contractors including new hires.

Course Objectives: At the end of the course, employees 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
- Identify and report suspected or actual loss of personal information.

B. **Course name: Global Information Security**

Course Description: This course instructs employees on how to secure Align’s personal information.

Target Audience: All pertinent current employees and contractors, including new hires.

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

- Understand why data protection is important to Align;
- Comprehend how and when to secure Align’s people, information, assets and facilities;
- Comply with information security expectations internally, when acting as a vendor and when appointing third party vendors to act on Align's behalf;
- Distinguish confidential data from public data; and
- Know where to go for assistance.

APPENDIX 2

DATA PROTECTION BINDING CORPORATE RULES POLICY AUDIT PROTOCOL

**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 Counsel will be responsible for ensuring independent audits are performed that fully address the Policies. Align's Privacy Counsel will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of Align's VP, Corporate and Legal Affairs, and General Counsel 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 Counsel 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 Counsel, executive management, or the Board of Directors. The scope of the audit performed will be decided by Align's Privacy Counsel 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

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 Legal Department. Align's Privacy Counsel 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 Counsel and, if necessary, to the Senior Counsel, Litigation and Regulatory 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 Counsel 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. Align's Privacy Counsel will also be responsible for liaising with the European data protection authorities for this purpose.

APPENDIX 3

DATA PROTECTION BINDING CORPORATE RULES POLICY COMPLAINT HANDLING PROCEDURE

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 must 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 Counsel 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 Counsel, working in conjunction with Customer Service, will liaise with the applicable member/s of the Privacy Working Group, 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, Customer Service 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, a substantive response cannot be given within this period, Customer Service will advise the complainant accordingly and provide a reasonable estimate (not exceeding six months) 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 Privacy Counsel with resolving the complaint) or any aspect of a finding, and notifies Align accordingly, the matter will be referred to the Privacy Counsel who will review the case with another representative of the Legal Department and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The Privacy Counsel will respond to the complainant within six months of the referral. As part of the review the Privacy Counsel may arrange to meet the parties in an attempt to resolve the complaint.

If the complaint is upheld, the Privacy Counsel will arrange for any necessary steps to be taken as a consequence.

- 3.1.4 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.

3.2 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, 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.

APPENDIX 4

DATA PROTECTION BINDING CORPORATE RULES POLICY CO-OPERATION PROCEDURE

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

Co-operation Procedure

4. Introduction

1.1 This Co-operation Procedure sets out the way in which Align will co-operate with the European³ 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 Article 29 Working Party 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.

³ References to Europe for the purposes of this document includes the EEA and Switzerland

APPENDIX 5

DATA PROTECTION BINDING CORPORATE RULES POLICY UPDATING PROCEDURE

**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 European⁴ 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 Dutch data protection authority and to any other relevant European data protection authorities.

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 Counsel to consider, discuss with the affected client and resolve. If the Privacy Counsel 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 Dutch 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 Dutch data protection authority and to any other relevant data protection authorities of the reasons for any notified changes to the Policies.

⁴ References to Europe for the purposes of this document includes the EEA and Switzerland

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 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 Counsel 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.

5. New Group Members

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