Align Technology

Data Protection Binding Corporate Rules Controller Policy

Contents

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 ("**Group Members**"), a list of which is available at [www.aligntech.com], when collecting and using that information for their own purposes.

This Policy applies to all personal information of consumer, physician, employee and supplier data and Group Members must comply with and respect this Policy when collecting and using personal information for their own purposes.

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. When Align collects and uses the personal information of consumers, physicians, employees and suppliers 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[2] that do not ensure an adequate level of data protection. Some of the countries in which Align operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' data privacy rights.

WHAT IS ALIGN DOING ABOUT IT?

In order to comply with the law, Align must 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, employees and suppliers.

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 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 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 must 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 Counsel at the address below who will either deal with the matter or forward it to the appropriate person or department within Align.

[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.

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 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.

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 must 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 local law implementing the EU Data Protection Directive 95/46/EC 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 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 clear and comprehensive way (usually by means of a privacy statement) how their personal information will be used. The information they have to provide includes the following:

- the identity of the data controller and its contact details;
- the uses and disclosures made of their personal information (including the secondary uses and disclosures of the information); and
- the recipients or categories of recipients of their personal information.

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. 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 those purposes which are known to the individual or which are within their expectations and are relevant to Align.

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

Rule 2C – Align may only collect and use personal information collected in Europe for a different or new purpose if Align has a legitimate basis for doing so, consistent with the applicable law of the European country in which the personal information was collected.

If Align collects personal information for a specific purpose (as communicated to the individual via the relevant fair processing statement) and subsequently Align wishes to use the information for a different or new purpose, the relevant individuals will be made aware of such a change unless:

- it is within their expectations and they can express their concerns; or
- there is a legitimate basis for not doing so, as described in Rule 2A above.

In certain cases, for example, where the collection and use is of sensitive personal information, or where Align is not satisfied that the new use or disclosure is within the reasonable expectation of an individual, the individual's consent to the new uses or disclosures may be necessary.

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.

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 not excessive.

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

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

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

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.

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

European law expressly requires that where a provider of a service to any of the Group Members have access to consumer, physician, employee or supplier personal information (e.g. a payroll provider), strict contractual obligations, evidenced in writing and dealing with the security of that information are imposed, to ensure that such service providers act only on Align's instructions when using that information, and that they have in place proportionate technical and organisational security measures to safeguard personal information.

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5A – Align will adhere to the Subject Access Request 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 be supplied with a copy of personal information held about them (including information held in both electronic and paper records), together with certain other details such as their rights in relation to their personal information. This is known as the right of subject access in European data protection law. Align will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) when dealing with requests from individuals for access to their personal information.

Rule 5B – Align will deal with requests to delete, rectify or block inaccurate personal information or to cease collecting and using personal information in accordance with the Subject Access Request Procedure.

Individuals are entitled to request rectification, deletion, blocking or completion, as appropriate of their personal information which is shown to be inaccurate or incomplete and, in certain circumstances, to object to the collection and use of their personal information. Align will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR OVERSEAS TRANSFERS

Rule 6 – Align will not transfer personal information to third parties outside Align without ensuring adequate protection for the information in accordance with the standards set out by this Policy.

In principle, international transfers of personal information to third parties outside the Align entities are not allowed without appropriate steps being taken, 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.

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

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, health, sex life and criminal convictions. 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 express consent has been obtained unless Align has a legitimate basis for doing so consistent with the applicable law of the country in which the personal information was collected.

In principle, individuals must expressly agree to the collection and use of their sensitive personal information by Align unless Align has a legitimate 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 must be genuine and freely given and individuals do have the right to refuse to give consent. Where Align is reliant upon an individual's express consent to use sensitive personal information, Align acknowledges the right of an individual to withdraw their consent.

RULE 8 – LEGITIMISING DIRECT MARKETING

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

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

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 – Where decisions are made by automated means, individuals will have the right to know the logic involved in the decision and Align will take necessary measures to protect the legitimate interests of individuals.

There are particular requirements in place under European data protection law to ensure that no evaluation of or decision about an individual which 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.

SECTION B: PRACTICAL COMMITMENTS

Rule 10 – COMPLIANCE

Rule 10 – 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 11 – TRAINING

Rule 11 – 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 12 – AUDIT

Rule 12 – Align will comply with the Data Protection Binding Corporate Rules Policy Audit Protocol set out in Appendix 3.

RULE 13 – COMPLAINT HANDLING

Rule 13 – Align will comply with the Data Protection Binding Corporate Rules Policy Complaint Handling Procedure set out in Appendix 4.

RULE 14 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 14 – Align will comply with the Data Protection Binding Corporate Rules Policy Co-operation Procedure set out in Appendix 5.

RULE 15 – UPDATE OF THE RULES

Rule 15 – Align will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 6.

RULE 16 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 16A – 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 Counsel unless otherwise prohibited by a law enforcement authority.

Rule 16B – Align will ensure that where there is a conflict between the legislation applicable to it and this Policy, the Privacy Counsel will make a responsible decision on the action to take and will consult the data protection authority with competent jurisdiction in case of doubt.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

European data protection law states that the consumers, physicians, employees and suppliers whose personal information is collected and/or used in Europe by a Group Member acting as a controller and transferred to Group Members outside Europe must be able to benefit from certain rights to enforce the Rules and the appendices set out in this Policy as follows:

- *Complaints*: Individuals may make complaints to a European Group Member and/or to a European data protection authority of competent jurisdiction;
- *Proceedings*: Individuals may bring proceedings against Align Technology B.V. either in the courts of the Netherlands (being the jurisdiction of Align Technology B.V.) or the jurisdiction of the Group Member located in Europe from which the personal information was transferred to enforce compliance by Align with this Policy and the appendices; and/or
- *Liability*: Individuals may seek appropriate redress from Align Technology B.V. including the remedy of any breach of this Policy by any Group Member outside Europe and, where appropriate receive compensation from Align Technology B.V. for any 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.

- 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 Align Technology B.V.

PART III: APPENDICES

APPENDIX 1

SUBJECT ACCESS REQUEST PROCEDURE

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

Subject Access Request Procedure

1. Subject Access Request Procedure

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[3] have the right to be informed by Align whether any personal information about them is being processed by Align. This is known as the right of subject access.

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 the right of subject access and such subject access requests will be dealt with in accordance with the terms of this Subject Access Request Procedure ("**Procedure**").

1.4 This Procedure explains how Align deals with a subject access 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 subject access 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 An individual making a valid request to Align when Align is a controller of the personal information requested is entitled to:

2.1.1 Be informed whether Align holds and is processing personal information about that person;

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

2.1.2 Be given a description of the personal information, the purposes for which they are being held and processed and the recipients or classes of recipient to whom the information is, or may be, disclosed by Align; and

2.1.3 Communication in intelligible form of the personal information held by Align.

2.2 The request must be made in writing, which can include email[4].

2.3 Under normal circumstances no fee will be applied but this will be left to the discretion of the Align entity to which the request is made and in accordance with local applicable law.

2.4 Align must deal with a valid request within 40 calendar days of its receipt (or such shorter period as may be stipulated under local law).

2.5 Align is not obliged to comply with a subject access 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 subject access request where Align is a controller of the personal information requested

3.1.1 If any employee or subcontractor of Align receives any request from an individual for their personal information, they must pass the communication to Align's Customer Service immediately (or to Align's Human Resources if it involves a current, previous, or potential employee, intern, or contractor) 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 subject access request.

3.2 Initial steps

3.2.1 Customer Service (or Human Resources) will 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 Customer Service (or Human Resources) will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further

[4] Unless the local data protection law provides that an oral request may be made, in which case Align will record the request and provide a copy to the individual making the request before dealing with it.

information, if required, or decline the request if one of the exemptions to subject access applies.

3.3 Exemptions to the right of subject access for subject access requests made to Align as a controller

3.3.1 A valid request may be refused on the following grounds;

(a) Where the subject access request is made to a European Align entity 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

(b) Where the subject access request does not fall within section 3.3.1(a) because it is made to a non-European Align entity; and

(i) 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

(ii) 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

(iii) where the personal information does not originate from Europe and the provision of the personal information requires Align to use disproportionate effort.

3.4 The search and the response

3.4.1 Customer Service (or Human Resources) will coordinate with Information Technology and the relevant departments to conduct a search of all relevant electronic and paper filing systems.

3.4.2 Customer Service (or Human Resources) may refer any complex cases to the Privacy Counsel 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.

3.4.3 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 Customer Service

(or Human Resources) which includes the information required to be provided in response to a subject access request.

3.4.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort there is no obligation to provide a permanent copy of the information. The other information referred to in section 2.1 above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

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

3.5.1 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.

3.5.2 Certain data protection obligations are passed to Align in the contracts Align has with its clients and Align must 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 must 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 must 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.

3.6 Requests for erasure, amendment or cessation of processing of personal information

3.6.1 If a request is received for the erasure, amendment or cessation of processing of an individual's personal information where Align is the controller for that personal information, such a request must be considered and dealt with as appropriate by the local legal and compliance officer.

3.6.2 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 must be rectified or updated accordingly if Align is satisfied that there is a legitimate basis for doing so.

3.6.3 When Align deletes, anonymises, updates, or corrects 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.

3.6.4 If the request made to Align as a controller is to cease processing that individual's personal information 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 Counsel to assess. Where the processing undertaken by Align is required by law, the request will not be regarded as valid.

3.7 All queries relating to this Procedure are to be addressed to the Privacy Counsel.

APPENDIX 2

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 3

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 4

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 5

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 European[5] 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.

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

APPENDIX 6

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 European[6] 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.

[6] 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.